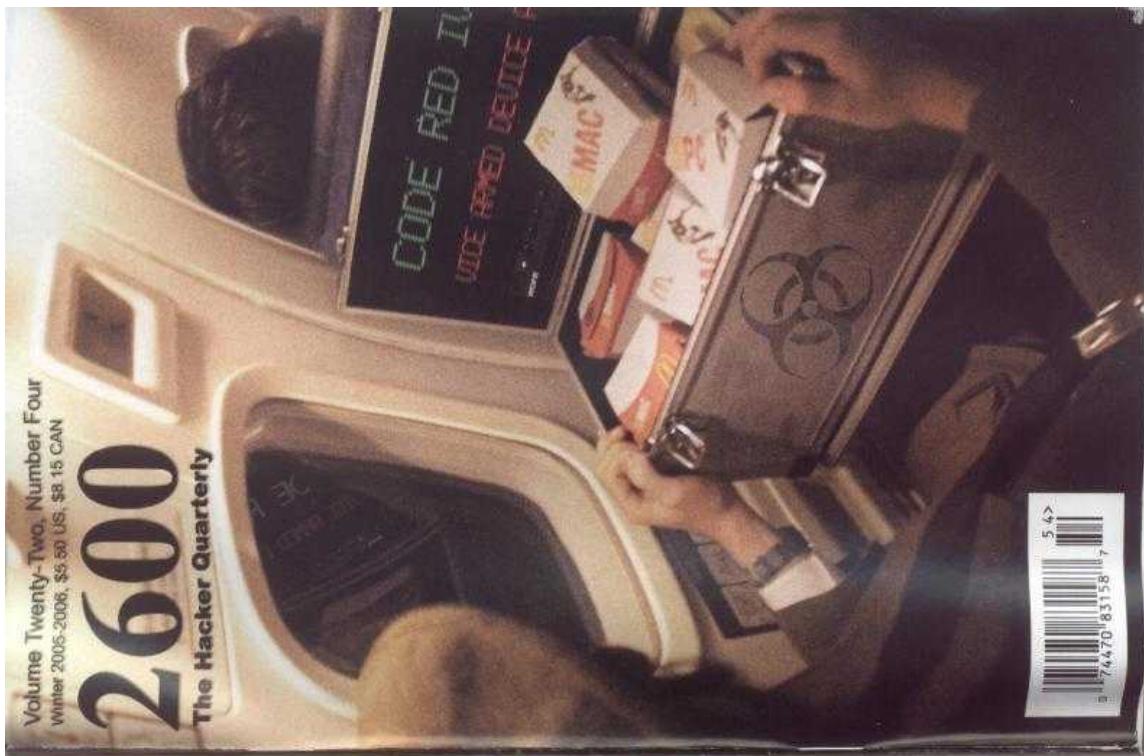
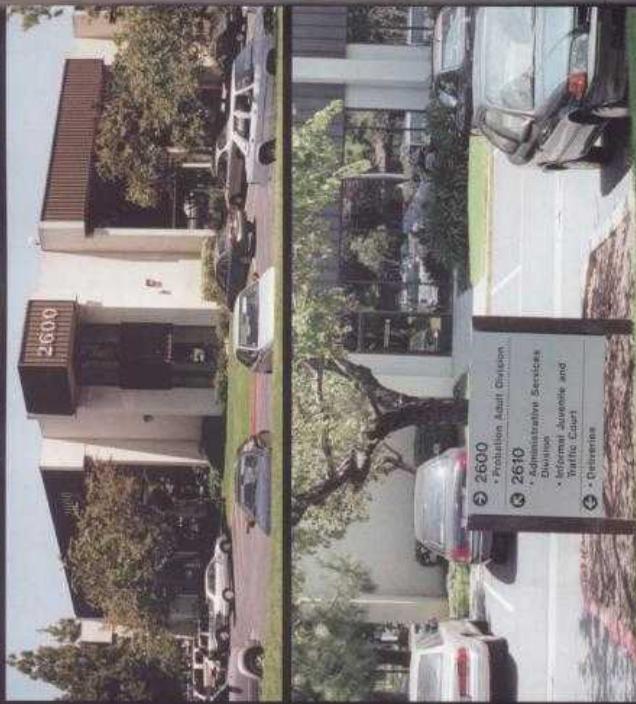


2600 Magazine – Volume 22, Number 4



The Back Cover Photo



Here's living proof that reading 2600 will lead to trouble. This little cluster of buildings in San Jose very subtly makes the connection. People driving by see the huge 2600 on the building and rush on over thinking that this is our legendary west coast distribution center. But when they arrive they get the message that becoming involved in 2600 will only wind up getting them sentenced as an adult.

Photos by Amore!

Do you have a photo for the back page?

Mail it on in to 2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953 or email it to us at articles@2600.com. (Yes, we know it's not technically an article but please humor us.) When taking digital photos, be sure to use the highest possible resolution. If we use your picture, you'll get a free subscription (or back issues) and a 2600 t-shirt.



North Korean Payphones!



In the lobby of the Yanggakdo Hotel, Pyongyang, this one only takes IC cards and makes local calls on the phone system that isn't connected to the outside world. North Korea has two phone systems - one is international-capable and the other can only place and receive domestic calls.

Photo by T/Prophet

Jordan



This phone doesn't take coins or cards and can only call local free numbers.

Photo by Eric

North Korean Payphones!



On the third floor of the Koryo Hotel, Pyongyang, this one has international capability. In use, you make an appointment for an international phone call (there are only three international circuits so all usage must be scheduled) and place your call, then, you pay when you're finished.

Photo by T/Prophet

Katrina



It's true that Katrina isn't a country and this phone isn't foreign. But it's definitely a payphone in a strange environment and a pretty sturdy one at that. We assume the receiver is around somewhere.

Photo by Cameron Buice

The Path to Knowledge

Preserving the Magic	4
Network Administrators: Why We Make Harsh Rules	7
Practical Web Page Steganography	9
Hacking a JP1 Remote Control	11
The RedBox DVD Kiosk	12
Punking the Watchers	13
How to Track Any UK GSM Mobile Phone	17
An Introduction to the Asterisk PBX	18
Spoofing Your Charge Number	20
Phone System Loopholes Using VoIP	21
Physically Accessing Your Apartment with Skype	23
Obfuscation and Encoding in PHP	24
AFOP Email Protocol - MD5 Challenge/Response	27
PGP Key Signing Observations	28
Letters	32
Persuasiveness and Social Engineering	46
The Real Electronic Brain Implantation Enhancement	47
Observing the Lottery	50
Sears Portrait Insecurities	51
Kodak Secrets and Wal-Mart Fun	53
The Workings of a Kodak Picture Maker	54
WiMAX, AT&T Style	55
Cheap Mobile Internet for Your PowerBook	57
Marketplace	58
Puzzle	60
Meetings	62

For more exciting foreign payphone photos, take a look at the inside back cover!

else who's doing the same thing. Nothing can deflate the sense of magic quicker than conformity.

And this is the problem that we have seen emerge. We take it all for granted and lose sight of the fact that these are true wonders of technology. And by losing that we also lose much of the inspiration that can lead us to much better advancements and new ways of doing things. Email isn't so much fun when you can't ever get away from it. And when using the telephone is something we do almost as much as we breathe, it somehow ceases to be exciting.

How many of us can say we remember what it used to sound like when making a long distance call? Even the term "long distance" used to have a different meaning and could apply to a destination less than 100 miles away. You could easily tell if you were speaking to someone down the road, in a different state, or on the other side of the country. And calls to foreign countries always had this air of mystique about them with the hiss of the trunk line, a slight echo, and the ever present in-band signaling tones. Telephone calls themselves used to be events. Phones rang with a commanding bell. You never knew who was on the other end until you picked it up. Even answering machines were rarities. A ringing phone simply coming over the lines was inspirational and exciting for people who were curious.

In fact, when we started publishing, having a computer of your own was an unfulfilled dream in many cases. This dream is what led so many of us to the world of hacking. By exploring the phone system and packet switching networks like Telnet, and Lynx, people were able to stumble upon computers run by companies, schools, governments, or other institutions. It was that period of discovery that inspired so many and was indeed itself a magical era in the hacker world.

In many ways we've gotten exactly what we wanted. Early hackers were very keen on communications and loathe to pay the evil Ma Bell for the privilege. Phone calls of the past cost an astronomical amount compared to the rates of today. Connecting overseas was almost unheard of because it would cost multiple dollars a minute. And now it's less than a dime a minute if that much. With VoIP it can cost next to nothing. It would appear that the cheap and global connectivity we once fantasized about has become reality.

And of course the phones themselves come with more and more extra features. It's become almost impossible to find a mobile phone that is only a phone. Odds are you will have a camera, mp3 player, organizer, and/or the equivalent of a small laptop attached to the thing you want to use to make phone calls. Naturally you will be able to transmit and receive the pictures you and other "phone users" take and those pictures will only get better looking as technology marches on. We've already entered the world of movies so in effect you may also have the equivalent of a small camcorder traveling around with you.

Oddy enough, the voice quality of a telephone call on one of these things is dramatically lower than something that's been around for many decades: a landline. The technology

much cheaper. But it's also very routine and mundane. The magic has been sucked right out.

Of course it would be ridiculous to resist advancement because of these nostalgic feelings. But we will be losing a great deal if we become so caught up that we fail to marvel at what we're actually doing when we communicate through technology. And not appreciating what it is that your computer is doing when you perform a routine task isn't much different than not understanding what's going on and becoming a mere user who will never stray from the norm or question the rules.

So how do we regain this sense of magic?

It's simple. As we believe what we're doing is exciting and can be shaped into something that nobody else has accomplished, our passion will be as strong as it ever was. This almost invariably means taking risks and doing things in ways that are very different from what we're told. That's what hacking has always been about and that's what continues to inspire people to become a part of this world.

It's the power of the individual to think

something, despite everything they're told

about how the only way to succeed is to be like

everyone else. This obviously is a basic tenet

of individuality, which can be applied to any

aspect of life.

For all of the positive advancements we

have witnessed, there is always a dark side.

Our society has become obsessed with surveillance and individuals have an increasingly

shocking amount of privacy to protect. While

we may have made our lives easier with satellite technology and the latest microscopic computer chip, you can bet that others have used this knowledge to create more efficient ways of killing and oppressing. And never before has the gulf between those who have a world of technology at their fingertips and those who have nothing been so vast. Not every advancement in technology is by default a good thing.

Our understanding and our passion have gotten us this far. We would be foolish to think that this is where it stops. As the people who design systems, find security holes, and constantly question all that we're told, we have a special responsibility to keep the whole thing magical, fun, and beneficial. We should never lose our link with the past. And we cannot let our link to the future be taken from us by those who don't know how to dream.

DITRA-TERRESTRIAL RELAYS the Magic

As Arthur C. Clarke once said, "Any sufficiently advanced technology is indistinguishable from magic." Anyone who's been on this planet for more than a decade would probably agree to some extent. So are we in fact living in a time of magic? Let's look at where we've come.

We can now stay in touch with everyone we know no matter where we are. And by staying in touch, we're talking about nearly everything imaginable. It was enough of a revolution when you were able to start using a computer that wasn't connected to a wire. But now you can also be connected to the Internet. Not just for rudimentary text content but full graphics as well. The speed continues to increase and soon will be indistinguishable from a home or office connection. Many of us walk around now fully able to instantly respond to any email sent to us regardless of where we happen to be standing.

And of course the phones themselves come with more and more extra features. It's become almost impossible to find a mobile phone that is only a phone. Odds are you will have a camera, mp3 player, organizer, and/or the equivalent of a small laptop attached to the thing you want to use to make phone calls. Naturally you will be able to transmit and receive the pictures you and other "phone users" take and those pictures will only get better looking as technology marches on. We've already entered the world of movies so in effect you may also have the equivalent of a small camcorder traveling around with you.

Oddy enough, the voice quality of a telephone call on one of these things is dramatically lower than something that's been around for many decades: a landline. The technology

is mirrored all throughout our society. Nearly every task

from typesetting a publication to

music to running a business - has been revolutionized by the magic our technology has achieved. And yet we seem to spend more time working at these tasks than ever before since the priority now is keeping up with everyone

"Value your freedom, or you will lose it, teaches history. 'Don't bother us with politics,' respond those who don't want to learn." - Richard Stallman

STAFF

Editor-In-Chief
Emmanuel Goldstein
Layout and Design
ShapeShifter
Cover
Dabu Ch'waid, Salido

Office Manager
Tampurf
Webmasters: Juintz, Kerry

Network Operations: css
Quality Degradation: mic
Broadcast Coordinators: Juintz, lee, Kobold, bsd

IRC Admins: shadry, r0d3nt, carton, beave, sj, koz
Inspirational Music: Bruno Nicolai, Alain Goraguer, Neotek, Los Aterciopelados, Autecine

Shout Outs: Hubert Cumberdale, Norm Prussin
Congrats: Aaron McGruder
Welcome: Lillias Faye
RIP: NinjaJicious

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc.
2 Flowerfield, St. James, NY 11780.
Periodicals postage paid at St. James, NY and additional offices.

POSTMASTER:

Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.
Copyright (c) 2006

2600 Enterprises, Inc.

YEARLY SUBSCRIPTION:
U.S. and Canada - \$20 individual, \$50 corporate (U.S. funds).

Overseas - \$30 individual, \$65 corporate.

POSTMASTER:

Back issues available for 1984-2004 at \$20 per year, \$26 per year overseas.

Individual issues available from 1988 on at \$5.00 each, \$6.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:

2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 (subs@2600.com).

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:

2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099

(letters@2600.com, articles@2600.com).

2600 Office Line: 631-571-2600

2600 FAX Line: 631-474-677

Network Administrators: Why We Make Harsh Rules:

The Piano Guy

The basic *driving* about writing another article for 2600 *got* quite some time. I didn't, however, because from at least some of your readers' perspectives, the other side of the line, "I am the guy in 'Management' who deals with folks that break the 'management' rules."

I figured it was time to write this article based on a letter from a user (22:3, Luke, like many letter writers, was a "student in school" who did "just a little hacking" that got paraded down to the principals office and suspended. What irked me enough that I decided to write this article is the immature SOB of a systems administrator who teased him. That bothered me a lot, since being that immature can't do anything but leave a bad taste with Luke. Lesser men would get revenge. I'm seeking peace through understanding.

I felt I needed to explain to those of you who don't get it how come network rules exist, and make it clear that we (i.e., management) aren't all out to get you. Instead, we are more concerned about covering ourselves and making sure that all network users can get what they need from the network, when they need it.

I work for a nonprofit that is a daughter agency to a larger nonprofit. One of the sister agencies has a brilliant man who provides our network connectivity and security. He also does this for several other of the daughter agencies. He sets the rules and I enforce them. We're all on the same big network.

For people who absolutely have to do stuff that isn't within these rather strict rules, there is a computer in a library that are hooked up through a different network, where security isn't nearly as tight. Then again, they are a few computers and they aren't all part of a domain. The general public has access to these computers, so my users can do what they want, on break, in our library.

To sum up, we have a lot of policies that restrict the use of the network to a great degree. However, if anyone needs to do something for business-related purposes, we find a way for them to do what they need. Either we change a rule, or we give them particular permission forever or for a distinct window of time. If you're on the "business side" of the network there are strict rules.

These rules are as follows:

1. Use the network for business purposes only.
2. No one hooks up other devices to the network without permission (i.e., laptops, PDAs, thumb drives, wireless peripherals, etc.).
3. No one installs their own software or does installs besides me.
4. No one connects to personal email, either through a software client (i.e., Outlook Express) or through a web interface.
5. No one uses chat software.
6. No one uses file sharing software (i.e., Kazaa).
7. No use of Internet radio or downloading of music or video files, unless related strictly for work purposes.
8. No copyright infringement.
9. No attempting to circumvent the current security systems or hacking.
10. We make it clear that we offer no expectation of privacy on our network.
11. All executable and zip files are blocked at the firewall.

Some of that may seem reasonable to some of you, and some of that may seem way over the top. There is a reason for each rule, however. Explaining the reason may make it both you less when you encounter one or more of the rules in your daily lives as employees or students.

First, we are understated. It is all I can do to do my day job without having to chase down viruses too. That, and my virus hits one of my machines could easily hit all of the machines in the network. As an example, Sircam was certainly very good at jumping from machine to machine. One user making a bad move can infect literally hundreds of computers, requiring hundreds of staff hours to clean up the mess. It could literally cost six figures worth of labor and lost revenue to recover from one user's mistake. So we set policies and hardware in place that make sure that that one user isn't likely to make a mistake.

As an aside, when I use "virus" in this article, feel free to plug in Trojan, ad-ware, spyware scumware, or worm, or what have you.

Second, we are under budgeted. We are non-profit in every sense of the word. It would be great if we had the money to buy more bandwidth, more staff, and better protection, but we just don't. Third, while most of the users are bright

people, some of them have trouble finding the on/off switch. I have to support them regardless, so there are rules exist to cover us for the lowest common denominator.

For these reasons, we insist that the network be used for business purposes only. Users going to business-only related websites reduces significantly the chances of them coming across a virus, and it does reduce our bandwidth usage. If someone is doing something personal and not causing a problem, we probably aren't going to even notice. If they are causing a problem, we need to be able to tell them to stop, and have policy on our side.

By restricting connections of PDAs, laptops, and thumb drives to our network, we prevent yet another vector of viruses onto the network. Yes, there are people who do use thumb drives and PDAs and laptops. The PDAs we approve are not Internet-capable. Laptops have current anti-virus software (and I check this to make sure they keep their subscriptions and definitions current). Thumb drives are brought to me to be scanned for viruses before being connected to the broader network. Or, maybe they are not. If a thumb drive is not brought to me, is connected, and the network is infected, then at least we have grounds to terminate the employee.

The restriction against bringing in one's own software for install is threefold. First, someone downloading software doesn't know that it is virus-free. Second, if someone wants to bring in a program from home that they want to use in both places, that is a violation of copyright law, which puts our agency at risk for fines. Third, if it's on one of my machines, then I have to support it. That may be a hassle (because the program might be horrible), and it may interfere with other software on the computer. I just don't have time to chase down these kinds of problems. It is better if a user needs something that we find an agency-wide solution for the problem, even if it is only one person that needs to do it. Sometimes many people have to do the same thing. I can better support it if they all use the same method and tool. This helps keep standards too, so everyone is doing something in an efficient way that doesn't mangle the network.

Not bringing in email from outside or using chat software is simply the prevention of a virus vector. Reduced use of bandwidth is an added benefit, but it pales in comparison to not getting a virus on the network.

Not using Kazza and its ilk covers us for bandwidth, virus prevention, and copyright infringement.

Not downloading media files saves us from

copyright infringement. Our marketing department does bring media files onto campus, and we do use them. They are intimately aware of the files on most of the clients (we're running W2K, not XP). If someone needs to get something via zip, we ask the person sending it to rename the extension. Then it comes through. Someone sending a virus isn't going to do that. My users who have a need to receive zip files ask for them to be renamed, get them, rename them back, and scan them before opening. These are my "bright build" users. As a result, I've never had a problem with a zip file virus.

In essence, we have these rules to protect us from network damage, and to make sure that everyone can do what they need to do when they need to do it. The rules are not to punish hackers. They are to make sure that hackers don't accidentally punish other users.

WRITERS WANTED

2600 has always been a digest of information from the hacker world. That means people who may be almost exactly like you. Or, it could actually BE you. Yes, you. If you have interest and knowledge in a particular field related to technology, communication, privacy, or security and you also possess some degree of literacy, you have most of what you need to get an article published in 2600. In fact the only other thing you need is the article itself. But don't let that intimidate you. Just remember to keep it interesting and hacker related. Don't be afraid to go into a lot of detail. Too long is better than too short since we can always edit it down if necessary.

Send your article to articles@2600.com (ASCII text preferred, graphics can be attached) or mail it to us at 2600 Editorial Dept, PO Box 92, Middle Island, NY 11953-0099 USA. If you go the snail mail route, please try to include a CD copy so we don't have to retype the whole thing if we decide to use it.

Articles must not have already appeared in another publication or on the Internet. Once published in 2600, you may do whatever you please with your article.



Practical Web Page Steganography

RGB, ISO 8859-1, and 1337sP33K

by Gutton

The idea as it's traditionally presented is this:

Steganography is Greek for "hidden writing." The concept has actually been around for ages, with the idea that adding a "security by obscurity" layer to an encoded message would make it even harder to crack. There are legends of Greeks covering hidden messages in wax or writing it in invisible ink. In our day we tend to think in technological terms. There was a rumor that the 9/11 hijackers used digital steganography to communicate, but this was discovered to be totally untrue. Stego even made it into a Hollywood movie, with Morgan Freeman using it in *Along Came a Spider*.

A 24 bit JPEG has eight bits for each color. If you swap out one bit for each pixel, you can use that bit to hide data with a negligible loss of color. All very interesting, but not practical because of the need of specialized software. Plus often times web-based images go through some sort of resampling, resizing, or compression. For example, if you upload an image to eBay, you don't see the original photo in your listing. You see a copy of it. Whether this affects the functionality of the stego or not is unknown but nevertheless it adds to the worry. Then there is the fact that the authorities have exhaustively researched steganog-

raphy because of the supposed 9/11 connection. They probably have image-sniffing bots snoopering the net, searching for those tall tale dropped bits.

RGB Stego

There is an easier way. Computers display color using Red, Green, and Blue with each of the three colors represented as a value between 0 and 255. As it happens, this is also the range for the standard ISO 8859-1 character set that is embedded in all TrueType and Type 1 fonts. For example, 36 is the code for \$, 91 have a single pixel of color, with the value of R=99, G=97, and B=116. Well, with that one pixel, I spelled "cat"! With three bytes per pixel, you can fit an incredible 15,552 characters into a typical one inch square graphic!

Before you get all excited, here are some difficulties. First, unlike the dropped-bit stego, that one by one image won't look like anything except mush. Second, without specialized software, it would take forever to encode a 15,000 letter note in Photoshop! It would also be a drag to decoder you'd have to open the graphic in Photoshop and check the RGB values for every pixel. And finally, once the bad guys figure out what you're doing, they can decode your message as easily as your intended audience can.

Before I get into possible solutions, here are a couple of other ideas for concealing messages on the web. This is merely text appended to a file, visible or not depending on the processes used. The technology was developed in association with a couple of newspaper groups in order to embed copyright data, cutlines, credits, and so on. Digital cameras add a record of their model number and sometimes f-stop and ISO settings to metadata. In Windows, you can edit this information for files saved in Photoshop, TIFF, JPEG, EPS, and PDF formats. In Mac OS, you can add file information to files in any format. The text is embedded in the file using a format called extensible Metadata Platform (XMP). Now how does this help us? Well, there is room for comments among the fields, so short messages could be attached to Jpegs and placed on a web page. For this to work, you'd need to have a prearranged plan for which image to nab. Maybe you have an album of innocuous vacation photos but one special one in which you have embedded the message. Since anyone can look at metadata if they know how, you could even encrypt the data for added security. Now, why not just email the data on using PGP? Well, if the bad guys intercept an email containing an encrypted message, they'll know you're up to no good. Sneaky is good.

HTML Stego. Even easier than RGB steganography, HTML's color palette can be used to create ranges of 0 to 255. In the good old days, there were a finite number of colors that everyone could view on the web. So, colors were and are represented by six hexadecimal digits - FFFFFF is white, for example. The first two digits are Red, the second two are Green, and the final two digits represent Blue. Sixteen times sixteen equals 256, and there you have your character ranges. All you have to do is create apparently decorative blocks of color using the <table> feature, but these are actually your hidden message. Or you could color snippets of text with your code colors, requiring readers to View Source to see their values. The advantage of HTML steganography is that you don't need anything but your wits and a text editor to encode or decode!

Solutions To Problems

Mishap: You coded RGB message looks out of place on your web page. Shrink it down to one pixel by one pixel and it will be an innocuous dot in one obscure corner of your page. Or float a butt ugly logo over it using CSS layers. Or make the coded portion of your message a strip of pixel wide at the bottom of your decoy image.

Time Consuming: I mentioned the 15,552 characters to illustrate, but your message need not be *Way and Peace*. A simple message of 120 characters would need only 40 pixels. If you were really ambitious, you could write a program that analyzes the color values of graphics and returns as outputted text a string of 0-255 numbers.

Insecure: Simply scramble the ISO 8859-1 character set, and voila! You have a substitution cipher. One of the weaknesses of a substitution cipher is its susceptibility to being cracked by guessing the letters based on their frequency. However, those ciphers are based on a 26-letter hash. We have 256 characters! So how can we use this to our advantage? Well, how about our native language of 1337/s337? Don't groan, there are numerous glyphs in the ISO 8859-1 character set that resemble other letters. Take the most easily guessed letter, E. We can substitute 3, É, è, Ê, ë, and so on. All perfectly readable once decoded, but to the codebreaker trying to crack a substitution cipher, it's a huge stumbling block. Or of course you could encrypt the message with PGP and make it all but unbreakable.

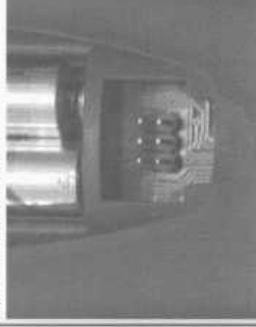
Conclusion

Sometimes the most difficult code to break is the one you can't see. While not perfect solutions, the ideas presented here can help keep your communications private in a world in which someone, it seems, is always watching and listening.

Hacking a JP1 Remote Control

by J.M.

Have you ever seen a connector like this labeled "JP1" on the back of a remote control and wondered what it was for?



Now create a folder and extract IB515.zip to it. Then create a subfolder called "RDF" and extract the contents of the R0f2.zip file to that folder. The first time you run IR, go under the File menu and select "Set R0f Path", and select the R0f folder you just created and extracted the files to.

With IR.exe you can download and modify the settings from your remote, as well as create backups of your remote's settings so if anything happens to the remote and it loses its memory, you can easily reprogram it with all of your customizations. And depending on your remote's capabilities, you can modify things like key moves, macros, learned signals, device upgrades, and more.

To create upgrades for the remote, or to use upgrade files, other people have created, you will need a Java program called RemoteMaster. First, download and install the Java 2 Platform (J2SE) version 1.4.1 or later from <http://java.sun.com/j2se/downloads/>. Then download RemoteMaster from <http://www.hifir-remote.com/forum/thread.php?sourceforge.net/>.

To execute RemoteMaster, open the file "RemoteMaster.jar".

Finding and Using Device Upgrades

You can find device upgrades that other people have already created in the "Device Upgrades" section of the JP1 File Section forum (<http://www.hifir-remote.com/forum/thread.php?sourceforge.net/>). One note: You have to register and be logged in to see anything in the list.

Once you find an upgrade you want to use with the remote, run RemoteMaster, open the file "RemoteMaster.jar" and open the upgrade file. With the upgrade file open, select the model of your remote control in the drop-down menu at the top of the window. Now click the Layout tab and make sure the remote buttons are oriented with the correct functions. To change what function is assigned to a button, right-click it and select the function you want.

Once you have everything in RemoteMaster set the way you want it, click the Output tab. This is the data that the IR program will use. Click the copy button and go back to IR. In the IR pro-

gram, under the Devices tab, click the Add button. In the window that appears, paste the data you copied from RemoteMaster in the top textbox. Then just say OK. Now all you have to do is assign the upgrade's setup code to one of your remote's device keys and upload the settings back to the remote.

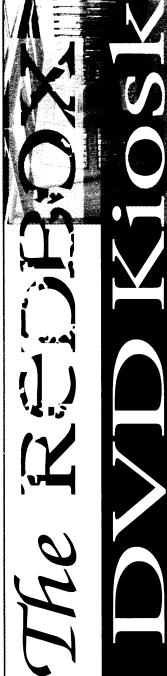
How to Create Your Own Device Upgrades

If your remote has a learning feature, you can also use IIF and RemoteMaster to create your own device upgrades. If you can't find one that works with your device, Once your remote control has learned the keys you want to put in the device upgrade, download the remote's data with IR. Under the Learned Signals tab, click one of the buttons you want to use with the upgrade and note the button's Protocol and the Device Code. Then go back to RemoteMaster and change the Protocol and Device code to match what you got back to the remote.

Conclusion

For the function you want to create and enter it into the Functions list in RemoteMaster.

When you enter one of those three numbers into a function in RemoteMaster, it will calculate the rest. Once you create all the functions you need, just map them to the buttons like you did before and copy the output to IR. Then just set up a device that uses the Setup Code you assigned to the upgrade and you're done. If you create a device upgrade you think someone else may have a use for, you can share it by uploading it to the "Device Upgrades" section of the JPI File Section



by blakmac

www.page33.com

Many of you may have seen or used the DVD rental kiosks that have taken up residence at many McDonald's restaurants. The machine at our location, a RedBox model DVD-01, provides an extremely easy and affordable way to rent new release movies, provided of course you have a valid form of plastic payment. In this article we will look at what could be considered a major security threat if applied properly, as well as address some theories which may or may not be founded in reality. If you are in need of a disclaimer, stop reading right now.

The Machine

The RedBox model DVD-01 is more or less an off-the-shelf computer running Windows XP Professional, some DVD dispensing hardware, and a touch-screen monitor in a big red metal box. The top section of the box houses the screen, DVDs, and all the mechanisms used to dispense the movies, whereas the lower section houses the PC, keyboard, etc. All of this can be considered boring to most of you. Oh, I almost forgot - this machine has a high-speed Internet connection. We will get to that shortly.

The Software

The RedBox software is launched automatically (I assume) on startup. As of this article, I have not found a way to exit the program. There is a "hidden" screen that asks for a username/password, however I've had no luck with that either. To access this screen, simply touch the "Help" button and then tap on the RedBox logo at the bottom of the screen. I assume that there are some interesting features beyond this login prompt.

Some other programs that run on this machine include programs to hide the start bar and one that looks particularly interesting - test controls for the DVD dispensing mechanism. This program did not have any information in the title bar, so more research is needed. Odds are that this program has a shortcut in the start menu, like the start bar hiding program (and several others that I did not have time to note - more information when I get it).

The Flaw(s)

Although I have so far been unsuccessful at

from the entry in IR. One last thing: Assign the corner of the screen and get (shock) a start menu. The start menu contains many (if not all) of the features you would expect from shiny new XP box, including games, miscellaneous software, and a wonderful feature for touch screen abusers called on-screen keyboard. This program has been part of the Windows Accessibility package for a long time, but since the keyboard is locked away in the bottom of the machine, this will help us on our journey. On the machines I have encountered, the screen is a bit insensitive so this is an annoyingly slow way to access things. But, patience is a virtue, right?

We'll start by launching the onscreen keyboard. After that, fit the bottom left corner again and then launch Internet Explorer. From here you can use the onscreen keyboard to access your favorite sites. (2600.com, page33.tk, etc.). Now wasn't that stupidly easy? You could also, of course, browse the hard drive of the system either from IE or My Computer (that's right, it's wide open). There may be things of interest such as user guides, but for the sake of conspiracy (this is speculation, but you never know...) since this is a machine that processes credit card transactions, there could possibly be logs of these transactions stored locally on this PC and, as we have demonstrated, virtually nothing to prevent someone from emailing files from this machine (using gmail, hotmail, or the like) to him/herself or to someone else.

Which brings me to another point. Here we have a machine that has complete http access to the Internet. Something else I have noticed about the RedBox is that most of the software maintenance is done remotely via the Internet, courtesy of XP's remote administration feature (which as far as I can see is always enabled since there isn't usually a technician anywhere around when this maintenance is being performed). So when this maintenance is being performed, So

here's a possible scenario: by obtaining the IP address of the machine, theoretically one could gain access via the remote admin tools. Another scenario is that one could download and install some kind of backdoor program, ftp, or http server on the RedBox itself, then gain access from a remote location. Either way the possibility of remote access exists.

Aside from this, one could manage to spawn a DOS shell using the techniques mentioned above (onscreen keyboard) and possibly gather information on other machines on this network. After all, they all must have a common server since you can return the DVDs to any kiosk and be credited for the return. (Browsing My Network Places was unsuccessful - I will be researching this further.)

Conclusion

Security through obscurity is not secure. I can't tell you how many articles I have read concerning touch-screen kiosks that have these same kinds of security flaws. Windows XP is capable of preventing these kind of problems (i.e., removing onscreen keyboard from the start menu, locking down My Computer, etc.) from happening. I hesitate to call these attacks because we are just working with the tools we are given. In fact, I'm not sure that finding these common flaws could even be considered "hacking," but I do know that thinking about obvious risks, creating theories, and testing ideas does allow someone to be considered a hacker.

Companies need to be more diligent in securing machines that process sensitive information before leaving them in a public place, allowing public access, and trusting everyone not to be curious about a big red shiny box.

Thanks to: Ximithan, ns_Sine, Greetings to:

briggs, carlos, Joe, nat, rebecca, Juan, and the rest of the Dayton McDonald's night shift!

Punking the Watchers

by Master Bojangles
cougar.stayer@gmail.com

I never had a real job before 9/11 so I was caught off guard by how paranoid people in corporate America have become about security.

What has always tickled me about this security is that you know its presence, but never are the details disclosed to you. Aside from the empty threat from HR that I am personally responsible for any outside software I install, they assume

Throughout the program, so get creative! I experimented with comparing two random numbers and changing the status when a match occurred. On a 1.5 GHz machine a range of one billion random numbers gave a suitable duration. Experiment on your own machine, but be mindful that too small a range and the status will change a hundred times a second, too large a range and the status will never change.

If you've ever seen the annoying "Program X is not responding... End Now or Cancel" box, this is a program interruption. Shutdown and Restart... what do you think they are? ForeLogoff... This one will be using programs the user out regardless of what other programs are done. So make sure you saved everything.

being snooped that they are a way of snooping. It's remarkable, but what about in the case of a Windows Forms application? I decided to deliberately use to manipulate the code whenever they are. As usual, I had to do some performance reviews, or any legal action as a result. The code is VB.NET, but could be another language that supports it. It will build a Windows Forms application in Visual Studio or for some command line compilers for the .NET Framework.

VB6 (#, J#, and J-script).
First, let's look at the Windows Form (Fig. 1) associated with this app. Only one value is accepted which is a number that becomes a number of minutes. The Go button starts everything. Notice the properties of this form (Fig. 2). The maximize box is not enabled. This prevents a clumsy user from accidentally filling the screen with this window just as the boss walks by. By setting ShowInTaskbar to False, this program very easily becomes invisible. Minimize the program using the appropriate window control and the app will still run but disappear (nearly) completely. Alternatively, the small window could easily be hidden by a larger one.

Now let's get into the code, starting from the `Run` method. System.Math is necessary for random numbers. The first `Private` statement is a declaration of the `ExitWindowsEx` function from the `user32` library (a system library) which is what forces Windows to close (or log off, more on this later). Next is the declaration of the `Sleep` subroutine from the `kernel32` library, another system library. This is used to tell the program to wait for a specified number of milliseconds. The `Sleep` subroutine is useful because it avoids the Timer control available in form design, which is only good for about a minute anyway. Next is the instantiation of the Windows Messenger API. Before this will work, you must add a reference to Windows Messenger, which is easy in Visual Studio. Go to the Project menu then Add Reference. Next, click browse and navigate to `mssns.dll` (should be in the `c:\Program Files (Messenger)` and the necessary reference is now included in your `.exe` file, so if you need to customize this for your own app, try adding it as a reference to a Visual Studio project and use the Object Browser to see what methods are available!

Next, the `Run` method handles the four different types of exiting Windows. Logoff does just that, however other programs are allowed to

Page 14

```

Public Class Form1
    Inherits System.Windows.Forms.Form
    Private Declare Function ExitWindowsEx Lib "user32" (ByVal uFlags As Long, ByVal dwReserved As Long) As Long
    Private Declare Sub Sleep Lib "kernel32" (ByVal dwMilliseconds As Long)
    Private WithEvents Winhook As Messenger
    Private Sub Winhook_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles Winhook.Click
        Logoff = 0
        Shutdown = 1
        Reboot = 2
        ForceLogoff = 4
    End Sub
    Private Sub Me_HelpClick(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles Me.HelpClick
        Dim Line As String
        Dim checkTime As Boolean
        Dim systime As Date = Dateime.Now
        Dim posTime As Date = Dateime.Now
        Dim randPos As New Random(CInt(Now.Ticks And Integer.MaxValue))
        Dim randPos As Integer
        If Line = "" Then
            Line = "Logoff"
        End If
        If checkTime Then
            If Line = "Logoff" Then
                ExitWindowsEx(1, 0)
            End If
            If Line = "Shutdown" Then
                ExitWindowsEx(2, 0)
            End If
            If Line = "Reboot" Then
                ExitWindowsEx(3, 0)
            End If
            If Line = "ForceLogoff" Then
                ExitWindowsEx(4, 0)
            End If
        End If
    End Sub
    Option Explicit On
    Imports System.Math
    End Class

```

```

position = Cursor.Position()
checkTime = IsNumeric(txtVal.Text)

If (checkTime = True) Then
  If (txtVal.Text > 0) Then
    time = txtVal.Text
    time = Now.AddMinutes(time)
  Else
    prime = MsgBox("Value must be > 0. Try again..")
    txtVal.Clear()
    Exit Sub
  End If
Else
  MessageBox.Show("Value must be numeric. Try again..")
  txtVal.Clear()
  Exit Sub
End If

Do Until getTime = systime
  systime = Dateime.Now

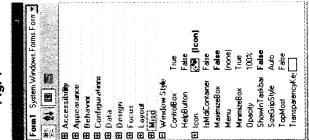
  Select Case systime.Second
    Case 15, 59
      randoos = rand.Next(0, 640)
      randpos = rand.Next(0, 1000)
      Cursor.Position = randpos
      Sleep(2000)
    Case 30, 45
      randoos = rand.Next(0, 480)
      randpos = rand.Next(0, 1000)
      Cursor.Position = randpos
      Sleep(2000)
  End Select

  Select Case systime.Minute
    Case 8, 26, 39, 46
      prime = MsgBox("Value must be > 0. Try again..")
      txtVal.Clear()
      Exit Sub
    Case 6, 23, 36, 44
      prime = MsgBox("Value must be > 0. Try again..")
      txtVal.Clear()
      Exit Sub
  End Select
End If

```

Inter 2005-2006

Eig. 1



-19.-

Clicking Go sets everything in motion. After the declarations, the first thing we need to do is set an instance of the Messenger API, which is done with the New statement. Cursor position is initialized and IsNumeric is used for error checking. If the value is numeric, it returns true. Next, the time at which to log off (gofftime) is set after passing the error checking.

The loop is the guts of the code. Based on the seconds in the current time, the cursor moves around a range of 60x60x60 sets as such for even the lowest resolution so an out of bounds will never occur. Note that a range can be specified with the New method of the random number generator. Then the program will sleep for two seconds. The cursor movement is just in case they are tracking user activity. The sleep is less trivial because it varies processor activity. This is useful for giving the appearance of a batch job running. In fact, in case they would check processor activity, the status of Windows Messenger is manipulated based on the minute of the system time. This serves to give the appearance of normal operation of status. True, this is formulaic, but it's much more that could be done here. From numbers provide a wealth of possibilities.

Page 14

How to Track Any

UK GSM Mobile Phone

(without the user's consent)

by Jonathan Pamplin

j.pamplin@gmail.com

As a result of improvements in mobile phone cell technology, UK mobile phone companies have for the past two years been able to sell transmitter data to online mobile phone location services which enable them to triangulate to within 100 yards the location of a given mobile GSM phone. This technology was in the news recently when the police tracked one of the London Bombers across Europe to his brother's house in Italy where he was arrested.

In order to be able to track a mobile phone and comply with the Data Protection Laws, mobile location services have to prove that the phone owner has given their consent to be tracked. They do this by sending an SMS to the phone's telephone number requesting a reply to the effect that you agree for the phone to be tracked. The majority of the phone location services only do this once to register the phone and then it can be tracked at any time without further SMS alerts to the phone.

This is all very well if you have access to the mobile phone to reply to the SMS agreeing to be tracked but that's no use if the phone is in the hands of someone else. Anyway it's not much fun tracking your own phone.

What I am about to describe is a way around this system which will allow you to track any UK GSM phone without the owner's consent on the following lines.

To begin with you need to set up an account with one of the mobile phone location services. I have chosen for this article <http://www.fleetonline.net> just because it offers a pay as you go service and does not charge you extra to add different phones as many of the others companies do.

I would suggest as a username you use something silly like "seygirsa" or "timebyanewphone" as the target phone will receive an SMS with your username in the beginning and if it's daß they will just assume it's just another junk SMS. You will also need to credit the account with 10 British pounds.

Now set up an account with one of the many fake SMS sites I've used (<http://www.sharpshorts.com>) and the user's consent. The recipient will get a message like this. You can see the message in the sent messages folder within Fleet online.

"BuyANewPhone 0735665432345 wants to locate your mobile from now on using FleetOnline, text 'T2Y' to 00447950081259 to agree."

"The important thing here is the reply telephone number 00447950081259 and the text "T2Y".

The reply number is always the same but occasionally the text changes to "T2X0T". You can tell if this is the case as you will see "*****" instead of "T2Y" in the sent messages folder of fleetonline.

Now go to your sharpmail account and send a fake SMS to the phone number you want to track to 00447950081259 with the text "T2Y".

Within a few minutes your fleetonline account will have registered that phone number and you will be able to track it to within 100 yards superimposed onto a detailed street map using fleetonline, all without the mobile phone user's consent.

If you have problems with the "T2Y" or "T2X0T" just attempt to register a random telephone number first. Then register the one you want to track and the reply code should always be "T2Y". There is no charge for adding new numbers using fleetonline so feel free to experiment.

This will work with many of the other mobile phone location services and fake SMS services.

Just use google to find an alternative if these let you down.

If you're concerned about being tracked using this method, use a Virgin SIM card as this is the only UK network not to provide tracking information to the mobile location services at present.

Although the current 3G services don't do it either, the fact that their handsets contain GPS suggests that they will be doing it soon!

Shorts to Nenma, Lynxtec, ServiceTec, and 4Mat.

```
End Select.

If optLine <= sysTime Then
    ExitWindowsEx(MinimizeBoxExitFlag, ForceLogoff, 0)
End If

Loop

End Sub

#Region " Windows Form Designer generated code "
Public Sub New()
    MyBase.New()

    'This call is required by the Windows Form Designer.
    InitializeComponent()
End Sub

'Add any initialization after the InitializeComponent() call
End Sub

'Form overrides dispose to clean up the component list.
Protected Overrides Sub Dispose(disposing As Boolean)
    If disposing Then
        If Not (components Is Nothing) Then
            components.Dispose()
        End If
    End If
    MyBase.Dispose(disposing)
End Sub

'Required by the Windows Form Designer
Private components As System.ComponentModel.IContainer
'NOTE: The following procedure is required by the Windows Form Designer
'It can be modified using the Windows Form Designer.
'Do not modify it using the code editor.
Friend WithEvents bando As System.Windows.Forms.TextBox
Friend WithEvents txtval As System.Windows.Forms.TextBox
<System.Diagnostics.DebuggerStepThrough()> Private Sub InitializeComponent()
    Dim resources As System.Resources.ResourceManager = New System.Resources.ResourceManager()
    Me.GetType().GetManifestResourceNames()
    Me.bando = New System.Windows.Forms.Button
    Me.txtval = New System.Windows.Forms.TextBox
    Me.bando.Location = New System.Drawing.Point(188, 5)
    Me.bando.Name = "bando"
    Me.bando.Size = New System.Drawing.Size(75, 24)
    Me.bando.TabIndex = 0
    Me.bando.Text = "Go"
    Me.bando.UseVisualStyleBackColor = True
    Me.bando.Location = New System.Drawing.Point(8, 8)
    Me.txtval.Name = "txtval"
    Me.txtval.Size = New System.Drawing.Size(177, 31)
    Me.txtval.TabIndex = 1
    Me.txtval.Text = ""
    Me.Controls.Add(Me.bando)
    Me.Controls.Add(Me.txtval)
    Me.Icon = CType(resources.GetObject("$this.Icon"), System.Drawing.Icon)
    Me.Location = New System.Drawing.Point(150, 150)
    Me.MaximizeBox = False
    Me.MinimizeBox = False
    Me.StartPosition = System.Windows.Forms.FormStartPosition.CenterScreen
    Me.Resizable = False
End Sub

#End Region

End Class
```


Your Charge Number

by greyarea@phreaksandgeeks.com

This has been controversial to people who understand the whole concept of Calling Party Number (CPN) and Automatic Number Identification (ANI). If you don't know the difference between the two, I can give an example to clear it up for you:

1. Peter calls my phone and I have it forwarded to Doug. Since Peter is the Calling Party Number, that will generate the Caller ID to Doug and Peter's number will show up on Doug's Caller ID display.

2. Peter calls my phone and I have it forwarded to NPA-555-1212. Even though he's the Calling Party Number, Directory Assistance will see my number because I'm the ANI. I originated the call to Directory Assistance and they will bill me. In each call Peter's ANI stopped at me and I became the ANI for both calls. But Peter remained the Calling Party Number. Got it? OK, let's move on.

There is proof that you can actually change the Charge number when spoofing. But it doesn't really change the ANI, just the Charge number. There are two different methods I'm going to talk about.

When you use the services of VoIP providers, the majority of them will let you choose your CPN (which as you know generates your Caller ID). That's not the ANI though because the call didn't originate from the number you chose. Some of them will set a ten digit non-billable number as your ANI so you can't charge someone else's phone with it and some of them will simply pass an ANI/FAIL behind your CPN. An ANI/FAIL is just a three digit area code that the call was homed out of.

There was an ANAC out there that read ANI instead of CPN and happened to be on the same backbone provider that one of my VoIP providers used. The number was 1-800-862-4622. (They noticed what I was testing and sent the DNIS to a VRU so it doesn't work anymore.) AT&T was the backbone provider. I could never spoof to this. I put together the theory that if you cross platforms (AT&T to Qwest) passing an ANI/FAIL as the ANI and setting your CPN, the receiving systems will recognize your number as the ANI. But they

don't because the ANI is still the three digit NPA the call was homed out of. But your CPN does become the Charge number if the number is a chargeable one without restrictions on the line. So since my provider uses AT&T, I have to call a Qwest number.

Some Qwest services that are vulnerable include the following: 1-866-YOU-TELL: Can spoof passing any ANI/FAIL and a valid CPN that is chargeable to call domestically and internationally. 1-800-888-7060 and 1-888-700-0400: Both these numbers are the same thing. They used to bill the CPN anyway but they recently fixed that. But they still didn't fix the problem when it came to spoofing the Charge number. They only fix when people are spoofing Caller ID. These will only allow you to call domestically and will bill the (billable) CPN you spoofed to it from the crossing platforms method. To call internationally off these you have to use another method: matching an ANI/FAILs, NPA to the NPA of the Charge number. This method you could even spoof to the 1-800-862-4622, which was pretty crazy.

Think of it like this. The systems are already designed to distinguish the ANI from the CPN. However, when you cross platforms with a fail as the ANI and set your CPN, then the receiving systems don't see the fail, only the ten digit number that passed and that becomes the "phantom ANI." When you match the ANI/FAIL's NPA to the CPN's NPA then that becomes the actual ANI. Even though the call was never originated from the number you chose, the receiving systems will place the CPN into the ANI fields and also the Charge number field as well. To test this, just spoof regular Caller ID to 1-800-CALLTNT with a provider that passes an ANI/FAIL behind your CPN and you will get the prompt: "AT&T, can I have the number you're calling from, please?" (The ANI they received was a fail.) Now find out what your provider is passing as the ANI in the ANI/FAIL and match it. Let's say it was 517. Set your CPN to 517-XXX-1337, call the same number again, and you won't get intercepted like you did before. You'll get them as though you had dialed from a regular PSTN phone.

Crazy, huh? Something to remember when spoofing, it matters who your provider uses for

their backbone services and who the service provider is that hands off the calls to the terminating number.

When I did the whole test on spoofing the Charge number, I made the charges to my house phone so that I wouldn't be charging up some poor noob's bill. This wasn't intended to be put out there for people to start charging other people's lines either. That's just plain stupid and gives you bad karma. It was put out to show how it works and the great vulnerability going beyond just spoofing Caller ID. Phreaking isn't getting free phone calls or any of that other shit. It's finding out how something works and recreating it yourself for making it better or more secure. But the key is being interested in how things work. Now with the knowledge of finding out how shit works comes the ability to place free calls and so on, but those types of decisions are up to the in-

dividual, not the phreak scene.

So in summary this is how it goes: ANI generates the Charge Number, Charge Number generates the Calling Party Number. Calling Party Number generates the Caller ID. You can change everything except for the ANI. When you change the Charge Number the system thinks it's the ANI but in the raw data that is being passed through SS7 it will still show the ANI as being a fail. But the receiving switch would have to be in debug mode for that to even be seen.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro, www.icon10.com, www.myslakodunia.com, www.cupospan.com, www.majestic.com, www.notthoery.com, and most of all [decooder.com](http://www.decooder.com). When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Shouts: www.oldskoolphreak.com, www.deafulradio.com, www.whitesword.ro

Physically Accessing Your Apartment

with Skype

by dopamine (Aubrey Ellen Shono)

First you will need to enter this code into your cell phone: "+21 *(NNN) NNN-NNNN#". (Replace the "Ns" with the number you are calling. The area code must be included.) Press "Send" after entering. Then dial your cell phone number from your home phone. You will now connect to the number you entered in the code. After the call is connected, dial "+#21#". (If you do not do this, anyone who calls your cell phone will be connected to the number in the code.) This is great for sending faxes, because it's really not convenient to send a fax with a cell phone. Just fax it to your cell and use the number of the line in the code.

This code is *not* the same as call forwarding. Forwarding a call using the phone's GUI usually uses a modified form of this code and can disable voicemail if used. The best part of this feature is that even though it uses your cell phone minutes, it will display the number of the phone you are actually calling from on Caller ID.

This works on most Nokia, LG, Motorola, and Samsung phones. There are a few models that won't accept the code, but they are very rare. (You can set up a script to send some of the basic data from your notification email to your phone as a text message, filtering out the unnecessary text to save space. This same trick can be used on some land lines that offer automatic forwarding after x number of rings. Note: can set valid information and also use your VoIP account to pick up incoming calls using your broadband Internet connection.)

Now let's say you or somebody you know lives in the U.K. Now you can have a U.K. number to make that situation more convenient. There is a site that will do this for you: www.uk2me.com

will assign a U.K. 0870 number to an existing U.S. cell/landline. Also, on the right you will see a link for "FWD 0870 Signup." This lets you set up a U.K. phone number for your FWD account. Don't use FWD? Get an Ipkall number for your current VoIP service (if it doesn't already have a U.S. phone number), then get a U.K. number for the 360 number you were assigned. Now you can get incoming calls from the U.K. to any VoIP service you want! Also, this service is needed if you want to check your Ipkall voicemail from a U.K. phone. You will need to create a U.K. number for the voicemail RX (360.515.3033).

Now you have a U.S. and U.K. number for your computer and you want to make outgoing calls

with your new 360 number. How do you do it? It's much easier than you think. All you need is a Caller ID spoofing service. Sign up for spooftel, camophone, etc., and you can make calls using your 360 number! This is great if you want people to be able to call you back from their Caller ID. Also, it can prove to be a lot of fun when used with *cough* other people's numbers....

Now the last part deals with pseudo-call-forwarding but not VoIP. This can be useful to know in relation to VoIP technology. If you have a cell phone you can use it for long distance plan on your home phone. If you want to make a call using your home phone (for better connections, longer conversations, etc.) you can easily use your cell phone minutes and pay nothing on your home phone.

First you will need to enter this code into your cell phone: "+21 *(NNN) NNN-NNNN#". (Replace the "Ns" with the number you are calling. The area code must be included.) Press "Send" after entering. Then dial your cell phone number from your home phone. You will now connect to the number you entered in the code. After the call is connected, dial "+#21#". (If you do not do this, anyone who calls your cell phone will be connected to the number in the code.) This is great for sending faxes, because it's really not convenient to send a fax with a cell phone. Just fax it to your cell and use the number of the line in the code.

This code is *not* the same as call forwarding. Forwarding a call using the phone's GUI usually uses a modified form of this code and can disable voicemail if used. The best part of this feature is that even though it uses your cell phone minutes, it will display the number of the phone you are actually calling from on Caller ID.

This works on most Nokia, LG, Motorola, and Samsung phones. There are a few models that won't accept the code, but they are very rare. (You can set up a script to send some of the basic data from your notification email to your phone as a text message, filtering out the unnecessary text to save space. This same trick can be used on some land lines that offer automatic forwarding after x number of rings. Note: can set valid information and also use your VoIP account to pick up incoming calls using your broadband Internet connection.)

Now let's say you or somebody you know lives in the U.K. Now you can have a U.K. number to make that situation more convenient. There is a site that will do this for you: www.uk2me.com will assign a U.K. 0870 number to an existing U.S. cell/landline. Also, on the right you will see a link for "FWD 0870 Signup." This lets you set up a U.K. phone number for your FWD account. Don't use FWD? Get an Ipkall number for your current VoIP service (if it doesn't already have a U.S. phone number), then get a U.K. number for the 360 number you were assigned. Now you can get incoming calls from the U.K. to any VoIP service you want! Also, this service is needed if you want to check your Ipkall voicemail from a U.K. phone. You will need to create a U.K. number for the voicemail RX (360.515.3033).

Now you have a U.S. and U.K. number for your computer and you want to make outgoing calls

tried just boxing it by holding a tone generator up to my mic for the first go-round. No luck. Computer microphones are pretty crappy these days.

The solution was a simple WAV editor. Most sound cards can use their own wave (software) output as a record input, so I recorded the tone from a software DTMF generator within the sound card, then added on my regular message with a mic. With a little editing, I had a nice message that sounds to a normal phone user like a tone followed by my voicemail greeting.

After creating the WAV file, just set your record input to your WAV out again, tell Skype to record a greeting, play the WAV file, then stop the record. Presto. You have a number you can call that will generate a predefined sequence of DTMF tones automatically without human intervention.

This trick would work just as well, of course, with a pbox card system that lets you buzz people in as long as you live there and can set the number it calls, or forward from that number. And it's a lot easier to misplace (and not have duplicates of) a pbox card.

Of course, the same trick would let you get into any apartment building where that lets you buzz people in as long as you live there and can set the number it calls, or forward from that number. And it's a lot easier to misplace (and not have duplicates of) a pbox card.

I figured I had three options. I could write a program to answer a call and send the correct tone using a modem or SIP. I could find another way to trick the door into opening (pink noise and the DTMF tone from the outside of the call box, maybe?). Or I could find a way to get DTMF into my voicemail message.

Luckily I just got hooked up with SkypeIn. Unlike other voicemail systems, this one lets me record a greeting from my computer. Still no upload for WAVs, but at least they don't stop recording on DTMF.

I had another problem. My area code has no SkypeIn numbers and I didn't think I could get my landlord to program a toll call into the box. Solution: Call forwarding on busy/no answer. Plus with my VoIP service, I don't pay long distance for the SkypeIn.

So with that, all there was to be done was to get the DTMF tone onto my voicemail greeting. I

Winter 2005-2006

2600 Magazine

Page 22

Page 23

Obfuscation and Encoding in PHP

Bryan Elliott

There are a few PHP obfuscators out there: programs that will take all the unnecessary comments, spaces, tabs, returns out of your code, then go further and find all the functions, variables, and classes that within the same scope mean the same thing, and change their names to something meaningless.

Indeed, these would make PHP scripts very hard to read. The result is often something like what happens when you compile then decompile a program in C. The English clues are gone, and you're left trying to figure out what i012 happens to represent.

Still, the code continues to be readable in a form. Run it through a code auto-formatter and you can at least trace what a program's going to do. It takes longer but it's still doable.

There are additional options here: one is that you can replace a given .php file with an encoded string that is processed and eval'd as the singular action of the include file. An example (remember that the .azm extension must be present):

To design an encoding I call phonetic64. Essentially it's base64. It uses the base64 encode built-in algorithm to get my six bit stream. I then translate that base64 encoding into numbers 0-63. From that I pick one of 16 consonants and one of four vowels to represent the base64 number. Just to switch things up and to ensure the sound doesn't get repetitive, I have values called 'oc' and 'ov' which are an unison consonant and vowel, each of which gets swapped with the last-used value in the substitution tables. For example, if something would normally decode to 'gig' and our oc+ and ov+, it changes to 'gifu'. As the data is encoded, spaces, punctuation, and even paragraph breaks are added to the stream.

Keep in mind that data encoded in phonetic64 is far larger than it needs to be. Consider that for every three eight bit bytes you're generating four six bit numbers and thus four word couples and 16 binary characters. This isn't even including the

available):
eval("?>" . gzuncompress(php eval("?" . ">" . gzuncompress(php eval("?" . ">" . base64_decode("([data])") ? ?
The `[data]` portion should be the contents
of the php file which has been gzcompressed,
then base64-encoded. An easy way to do this in
php is:

Here's the code for Phonic64.

```

function phpCompress($filename) {
    $data=base64_encode(gzcompress(join
        ("", file($filename)) . "eval(\"". ")\")");
    $data="".gzcompress(base64_decode($data));
    $data= fopen("obscured-", $filename);
    fwrite($data, $data);
    fclose($data);
}

Even on unmodified PHP code, an unscrupu-
lous fellow would have to decode the data him-
self (or, you know, replace "eval with echo" but
who's counting?). Still, the idea is to make more
obscure.

Anyway, this next trick was something that
came about when attempting to make pro-
nounceable passwords in PHP. I figured, "why just
generate random syllabants when you can have

```

age 24

2600 Magazine Winter 2005-2006

-Page 25

Proving Identity and Assigning a Check Level
 When signing keys, OpenPGP allows one of four levels of verification to be used with each signature. This allows a means of communicating the level of confidence the signer has gained in establishing the identity of the key's owner:

0 - No particular claim is made (generic certification)

1 - No verification of identity (persona certification)

2 - Casual verification of identity (casual certification)

3 - Extensive verification of identity (positive certification)

The definitions of verification levels are vague by design rather than by accident. This is a "feature, not a flaw, in the OpenPGP specification. What one person considers an "exhaustive verification," another person may consider little (insufficient) verification. Someone else may wish to read any message ever encrypted to Bob and sign any message or key with Bob's signature.

Aside from keeping his personal computer secure, Bob should save a copy of his private key in a secure, off-line, off-site location. This off-line and off-site backup keeps Bob's private key secure against loss from such things as disk crash or his computer being stolen by either common

or government thieves. Depending on who is out to get him, he may consider it more secure to burn his private key onto a CD and store it in a bank safe, or print it onto paper and hide it inside a painting. As always, the most appropriate meaning of "secure" is left to the needs and perceptions of the reader.

Note that it is often unnecessary to make a backup copy of a public key for two reasons: 1) if it's publicly available and can be retrieved from a keyserver and 2) the "gpgsplit" command has a "Secret-to-public" option that can recover a public key from a private key. Note that gpgsplit may not recover accurate expiration dates and preferences if they were updated after the key was created.

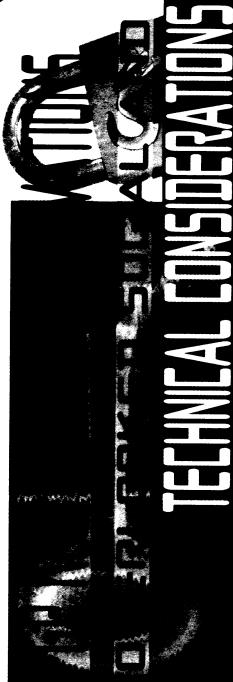
One should never sign a key (or use pgp at all) on an untrusted computer or in an untrusted environment. Gather the information needed to sign a key and sign it when you get home. If your home computer and environment are not trusted, you have bigger problems to worry about.

Requirements of Key Signing

One should generally consider signing a key only after the following three requirements have been met in a way that the signer considers acceptable: 1) The fingerprint of the key being signed has been accurately verified; 2) the owner of the key being signed has asserted (or preferably proven) that they "own" or control the private component of that key and; 3) the owner has proven that they are who they claim to be and their key represents them as such.

When Confirming Identity
 What if Alice and Bob know each other only through their work? They can produce identification in various forms (driver license, passport, work ID, credit cards, etc.) attempting to prove their identities to each other. If they consider this to be an exhaustive verification of identity, then they may choose to sign each other's keys with a verification level of 3. They may have known each other long enough that checking each other's identification seems unnecessary. The choice is theirs.

One or both of them might not trust any of the identification since they know how easy it is



by Atom Smasher

atom@smasher.org

762A 3B98 A3C3 90C9 6B7
582A B8BD 5224 DF5F 7808

While there are several sources of technical information on using pgp in general and key signing in particular, this article emphasizes social aspects of key signing that are often ignored, misleading, or incorrect in the technical literature. There are also technical issues pointed out where I believe other documentation to be lacking. It is important to acknowledge and address social aspects in a system such as pgp because the weakest link in the system is the human that is using it. The algorithms, protocols, and applications used as part of a pgp system are relatively difficult to compromise or "break," but the human user can often be easily fooled. Since the human is the weak link in this chain, attention must be paid to actions and decisions of that human; users must be aware of the pitfalls and know how to avoid them.

This article is intended to be of use to those wishing to participate in the exchange of signatures on their OpenPGP keys. It is assumed that the reader has a basic understanding of pgp, what it's used for, and how to use it. Those more experienced with pgp may wish to skip the sections they are familiar with, but it is suggested that even the basic information be reviewed.

Relevant Terminology

Alice, Bob, et al.: Following cryptographic convention, Alice and Bob represent two people who wish to communicate with each other. Trent is a trusted third party. Eve is a passive eavesdropper. Mallory is a malicious active attacker.

GnuPG: The Gnu Privacy Guard. This is an application that processes OpenPGP data. It is freely distributed under the terms of the GNU General Public License.

pgp: GnuPG.

OpenPGP: As defined in RFC2440, this defines

a message format concerning encrypted and/or authenticated data.

PGP (uppercase): This refers to a specific application that processes OpenPGP data. PGP is a registered trademark of whichever company currently owns the rights to it.

pgp (lowercase): Depending on context, this may refer to the OpenPGP protocol or any application that uses it, such as GPG or GnuPG.

signature: A digital signature of data. A signature of a pgp key is often called a certificate or certification.

secure: This is a subjective term that is frequently misused as an absolute term (similar to terms such as "easy" and "fast"). Used as a noun, "secure" means nothing meaningful unless it is qualified by an adjective. Used as an adjective, it means nothing meaningful unless it is qualified by an adverb. Something may be secure against fire, flood, eavesdropping, cryptanalysis, high explosives, alien technology, etc. It is generally believed that there is no such thing as absolute security, thus nothing may be considered absolutely secure. Only when a threat model is evaluated can one properly define what "secure" means in a given context. If "secure" is used without qualification, it must be interpreted by the reader based on their own needs and perceptions. If "secure" is used in an advertisement or press release, its meaning deserves suspicion and scrutiny.

UID: User Identification field. This is a component of a pgp key that contains information about the key's owner. Usually a UID includes both a person's (or group's) name and a valid email address where the person (or group) may be contacted. Optionally, a comment may also be included in the UID.

Observations on Generating and Maintaining Keys

When one first generates a key, it is important that it be done on a secure machine in a secure environment. One attack against pgp that is

to steal an identity or create a false identity. In this case one or both of them might consider that their signature only deserves a verification level of 0 or 2 depending on their confidence in determining each other's identity.

It is important to note that they do not have to agree on a level of verification for each other. Each of them may independently assign a level of verification to their signature.

Things Can Get Trickier When

Confirming a Pseudonymous Identity

What if Bob's key, instead of identifying him by his real name, identifies him as "The Bobster"? In this case, Bob is using a pseudonymous key. It is unlikely that Bob has any valid identification that can confirm this pseudonymous identity. It may seem like Alice shouldn't sign it, but that's up to Alice. If Alice can verify Bob's pseudonymous identity to her own satisfaction, then she may choose to sign his key with an appropriate level of verification (as determined by her). It is reasonable that Bob may earn a verification level dependent on how he is able to prove his identity. As always, if Bob wants Alice to sign his key, he has to prove to her satisfaction that he is who he claims to be, regardless of whether or not his key is pseudonymous.

It is important to note that some people may have strong reservations about signing pseudonymous keys. If you are using such a key, do not be offended if someone isn't comfortable signing it. Offer to sign their key anyway if they have earned your signature.

Last Word on Confirming an Identity

You are never obligated to sign anyone's key. You are never obligated to sign a key with a particular level of verification.

If you do choose to sign someone's key, they are obligated to prove their identity to your satisfaction. Only sign their key with a verification level that you are comfortable with. This applies equally to pseudonymous keys, anonymous keys, and keys using real names.

How to Sign a Key

Throughout the next several sections, references will be made to "key information." This is the information required to confirm that a key is not mistaken for a different key. At a minimum, this information must include the UID and fingerprint. For older style (v2 or v3) keys this information must also include key type (most likely RSA), creation date, and key size. Nearly all pgp

keys currently in use are v4 keys and it's generally considered acceptable to verify just the UID and fingerprint.

Using GnuPG, this command will display all needed information (except creation date) for Bob's key:

`gpg --fingerprint bob`

How to Sign a Key Under Ideal Circumstances

Ideally, if Alice and Bob want to exchange key signatures, they will plan an in-person meeting for this purpose. Prior to meeting, each of them will print their key information on a small piece of paper and verify that the printout is correct. When they meet, they exchange their slips of paper. If required, they may take this opportunity to present each other with formal identification. After enjoying each other's company, they each return home, verify each other's key information to be correct (between the papers they exchanged and the keys they are about to sign), and sign each other's keys. They may then exchange signed keys.

Alice and Bob Meet on the Train

Alice and Bob have been meaning to get together and exchange key signatures but their busy schedules haven't allowed this. Alice gets on the train where she's pleasantly surprised to see Bob. They weren't planning to meet and neither of them has their key information with them. This may seem hopeless but, after verifying each other's identification (to the extent they both consider necessary), they exchange a secret passphrase. When they get home, each of them will print their key information to a file and symmetrically encrypt this file to the passphrase known only between them. A command like this (on *nix) will export Bob's key information and use a passphrase to symmetrically encrypt it into a file:

`gpg --fingerprint bob / gpg -ac >`

Encrypt passphrase:

Bob can mail that file to Alice and, after decrypting the file (using the passphrase known only to them), Alice can confirm that she is signing the correct key. Alice uses the same method to send her key information to Bob.

In order for this protocol to be secure a passphrase must be "strong," must never be reused, and care must be taken that the passphrase isn't overheard (or otherwise made known) by anyone other than Alice and Bob. If Eve observes the passphrase being exchanged she may fool both Alice and Bob into signing the wrong keys.

Key Signing Parties

If you are hosting a key signing party, be sure to read len Sassaman's "Efficient Group Key Signing Method." If you are attending a key signing party, be sure that the host has read it.

Key signing parties are described on several websites, negotiating any need to discuss them here in any great detail. However, much of the currently available information on the topic is indeed insecure, breaches proper etiquette, or is just plain wrong. I suggest reading up on key signing parties to get a general idea of how they work, and then read the sections of this article referring to identity confirmation, etiquette, and exchange of signed keys.

Key Signing Etiquette

Usually (but not always), key signatures are mutually exchanged between two people. This is known as a reciprocal key-signing. This exchange usually (but not always) means that if Alice signs Bob's key, she expects Bob to sign her key. This may not always be practical or desired.

For any number of reasons (or no reason at all), Bob may not want Alice's signature on his key. An example might be a premature expiration date on the signature that Bob doesn't want. In order to accommodate this situation, proper key signing etiquette requires that Alice send Bob's signed key only to Bob. If Alice sends Bob's signed key to a keyserver, it will remain in public circulation indefinitely and Bob has no control over it. If Alice sends Bob's signed key to another user, it may find its way to a keyserver and become publicly circulated. If Bob wants Alice's signature on his key to be circulated, then Bob may upload it to a key server or distribute it as he sees fit.

For any number of reasons (or no reason at all), Bob may not want to sign Alice's key. In order to accommodate this situation, proper key signing etiquette requires that Bob does not immediately distribute Alice's signature on his key. Bob should first ask Alice if it's OK with her that he circulate her signature on his key even though he does not intend to sign her key. If Alice does not want her signature used without receiving a signature in return, Bob should destroy his copy of Alice's signature and not distribute it.

You are under no obligation to sign anyone's key or sign it with a particular level of verification. For any number of reasons (or no reason at all) you may not want to sign someone else's key. Just because someone has signed your key does not obligate you to sign their key. If they have signed your key and uploaded it to a keyserver, they have violated this etiquette. Their breach of etiquette does not place you under any obligation to sign their key.

Delivery of a Signed Key

As described in the section on etiquette, a signed key should be emailed to the key's owner. For enhanced security the signed key should be encrypted using the recipient's public key. Alice encrypts Bob's signed key to Bob (using Bob's public key) and emails it to the address in the UID of Bob's key. If Bob has more than one UID on his key with more than one address per key, Alice should sign each UID independently and send each signed UID to that address.

This provides one final test for Bob to prove his ownership of the key and accuracy of the UID: If Bob cannot receive or decrypt the signed key, Bob cannot (and should not) make use of that signature. This protocol is advantageous to both Alice and Bob. Alice is protected from having her signature circulated on a key with an incorrect email address or a key that is not controlled by a user of that address. Bob can review that the signature is acceptable to him before circulating it.

Delivery of a Signed Key

Between Untrusting Parties

Sometimes Alice and Bob may want to sign each other's keys but they distrust each other. This is a reasonable situation since signing a key is a certification of identity, not character. Neither of them wants to offer a signed key until after the other has done so first. There are several impractical protocols for solving this. The most practical solution requires the help of Trent. Both Alice and Bob send each other's signed keys to Trent. Trent will pass along the signed keys only after both of them are received. This prevents Alice from withholding her signature from Bob after Bob delivers his signature to Alice. Bigumber.com provides exactly this service.

If the above protocol is used, it may not be practical to encrypt the signed key to its owner. It is therefore suggested that an encrypted and signed email exchange be made prior to exchanging signatures, to ensure that the key and the UID(s) are correct.

Suggested Further Reading

Bruce Schneider, *Applied Cryptography*

Bruce Schneider, *Secrets and Lies*
Len Sassaman, "Efficient Group Key Signing Method" (<http://sion.quickie.net/keysigning.txt>)

"Alice and Bob" (http://en.wikipedia.org/wiki/Alice_and_Bob)
Atom Smasher's Open Source & Security Links (<http://atom.smasher.org/links/>)

Special proofreading and editorial thanks to:
Ed Moyie, Duane Dunston, and Seth Hardy.

guy this because I constantly see people whining about how slow their 1.0 ghz processor and 512mb of ram computers are. But yet they claim to be "hackers." A true hacker doesn't need a fancy 33000 box to explore the net and I just want to tell them to stop whining.

Thanks for hearing me out. I hope to read 2600 for years to come. Oh yeah, I'm sending this letter via mail from a Pentium 1 (speed unknown but slow) with 64mb of ram on Windows 95 and a shitty dialup connection (14.4kb) from my mom's house in the middle of nowhere. It took me three hours to configure it in order to get online just to send you guys this letter of appreciation for opening my eyes to the free information that I rightfully deserve.

Thanks for listening. At least someone does....

Mike
jpeg vrus

Dear 2600:

After borrowing 21:4 from an instructor at a school I was sent to, I was hooked. The articles were great and the cover was very intriguing. One of the many things your magazine has inspired me to do was learn the history. I think it's very important to know your roots and understand how it is a lot of things came to be today and in society. It's been very interesting reading articles and watching videos found online about Kevin Mitnick, Phisher Opt, and others.

Props to you guys. Keep up the great work!

At least the school you were sent to isn't that bad if the instructors are the ones reading a hacker magazine.

Mike

Dear 2600:

In the article titled "Javascript Injection" in 22:3, there is some HTML text in which the right angle brackets (>) have apparently been replaced with pipe symbols (|). I don't know why that happened, but it's astonishing that such a glaring mistake was not caught by the 2600 editors. It's not even the first time I see errors like that concerning HTML text in the magazine. Coming from a hacker publication, it's very disappointing.

George The Pancake
It's always sad when we let people down but there's no getting around it this time. We made a mistake. Hard as that may be to believe, it has been known to happen. Sometimes those particular brackets are temporarily changed when being imported into a program that uses those same brackets to interpret commands. This is an instance where they weren't changed back. We regret the error as well as the software.

Mike

Dear 2600:

I was just poking my nose through 22:2 when I fell upon an article labeled Remote UNIX Execution Via a Cell Phone." I have to say I became enlightened to a whole new world. You caused me to go pull a Dell out of my garage (crappy specs, like a 166mhz processor and 32mb ram but a network card is available) and install Slackware. Finding this remote system actually worked. I decided to step it up. So I wrote a few server applications, the first running on the Dell. This one routes the incoming data and sends it to the selected computer on my network. The rest, listen for the commands and process them. My network has an array of computers running Windows and others Linux, and now I am able to

netstat. Specifically, netstat with the -n0 option. This option lists every active port on your machine like netstat does but it also lists the processes tied to that port. So if it's using a port you will find where it lives very quickly here. Unless of course the spyware happens to include its own TCP/IP implementation!

savatus

Dear 2600:

We have reason to believe that your magazine published a bogus rack against SoniWall products in the Autumn 2005 article titled "Climbing the SoniWall." After analyzing the technique described in the article we attempted to contact Knighthawk in an attempt to verify his claims. As we have not received a response to our inquiries on how he was able to use a "nice little program that sniffs passwords" to defeat a 256 bit hash we have no choice but to assume that the author made false claims in his ability to compromise our security.

We believe that the article published in 2600 is a hoax.

Matt Dreyer

SonicWall

Dear 2600:

We intend to look into this and advise our readers to see if this is in fact untrue. Thanks for writing.

Advice

Dear 2600:

Two days ago I read about your work and I decided to search for it because I thought it was more than very interesting. I come from Spain, my English is not the best (but I hope I will be able to read your articles), but I would like to receive your magazine in a kiosk in my city because I am 17 and my parents don't like this type of education.

Javier

Parents everywhere are the same, aren't they? Getting us into a Spanish kiosk is a tall order since it's very difficult to get reliable overseas distribution in the first place. We will continue trying however. And when we succeed we'll update our list of stores which is on our website. We suggest subscribing to ensure that you get all of the issues in a timely manner.

Although I am comfortable enough to get around on a computer for word processing, Internet etc., I know that squat about programming and tech matters. On the other hand, I thoroughly enjoy the quarterly because of the insights I gain about the hacker's "mind." Thank you so much for presenting your material with this unique point of view.

For me, well, let's just say that after spending my adult life in higher education at traditional colleges and universities as a problem solver combined with a lifelong pursuit of metaphysical matters... I can certainly identify with the hacker's state of mind.

In that regard, perhaps you can advise me on the following personal goal:

There have been a lot of articles in 2600 recently with spyware detection methods that usually involve downloading some piece of software or another and a bit of debate as to which tool does the job best/better. I just wanted to point out, especially since Inglix the Mad mentioned Security Task Manager, that almost all copies of Windows have a tool built in, that does essentially the same thing and if you happen to be looking for spyware on a Windows box it's a good place to check. It's called

alphabot

Dear 2600:

1) Yahoo is working on the problem and a trouble ticket is open.
2) Yahoo has not been able to resolve the problem and the trouble ticket is closed.
3) You will have to call our cancellations department and uncancel your cancellation order; then, once uncanceled you can unlink the accounts and then recancel.
4) You cannot uncancel a cancel order.

2600 Magazine - Winter 2005 - 2006

Page 34

Page 35

5) There is nothing we can do to unlink these accounts. You will have to talk to yahoo directly.

I have talked with yahoo repeatedly and they say

there is nothing they can do and that it is something

that verizon must resolve.

I am further told by yahoo that if i do not successfully unlink the verizon account within 90 days they will delete my account.

I have had an account with yahoo for many many years. I would like to regain access to my yahoo account as it contains so much personal information, my personal calendar, my contacts list, cherished communications from the people I love, stock portfolio combos, that I track, etc. I can't even access my yahoo instant messenger.

Are you familiar with this problem? Might you have some suggestions or ideas about how to resolve this issue?

Phillip

You need to make friends with some of the people in these corporations. Your yahoo account doesn't have to be deleted and verizon can certainly be more helpful than they have been so far. But, despite the fact that they should have done a better job from the beginning, you will only get this fixed relatively quickly if you gain some allies on the inside. You can do this by getting their sympathy which is generally achieved by explaining the problem to as simple a way as possible. It may take a few attempts to get someone who can actually do something. You may have to talk to supervisors or techs. But it can be done.

It sounds as if hogging in to your old verizon account will fix the problem so that's probably the best path to follow. Obviously you can't do this since the account was canceled. But somebody at verizon most likely can. Yahoo can be made aware of the situation so that they don't delete your account. If you find the right person, they can really get a lot done for you. We've experienced this many times.

Of course things go badly, and as a last resort, you can always complain to the powers that be such as the local public utilities commission, the FCC, the attorney general's office, various consumer groups, and of course the media. But the trick in all of these cases is also to make it succinct as possible so the reader of your letter will instantly feel compassion for you and anger at those who are making your life difficult. If you get really steamed, you certainly could pursue a lawsuit. But that's also an investment in considerable time and money.

If and when things do work out, it would also be helpful to let the world know. You can be other people are experiencing the same type of problems on a daily basis. A search of the net reveals that you're not alone.

Dear 2600:

I have been reading your publication for many years and have picked up copies at national bookstore chains and small bookstores across the country. You guys are awesome. Your articles are always insightful, well written, and full of useful information. I only wish that more people would read it so that there could be a greater understanding of the service you provide to non-technical and technical people alike.

Unfortunately I am writing about a serious topic and I am hoping that someone out there can help with this

problem. Recently my sister's debit card was cloned and stolen. I can only speculate about the cloning since we have no idea what really happened. She had the card in her wallet when the illegal transactions occurred. The bottom line is that someone got a hold of her debit card number and the expiration date and used it to purchase \$900+ worth of merchandise. They purchased about \$550 worth of stuff from Wal-Mart and another \$300 and something from an electronics store. She only found out about the credit card transactions because the electronics store was kind enough to call her and let her know that something had been ordered with her card. The credit card company called her a few nights later to inform her that the purchases were made on the card. Okay, I'll say that again. The credit card company called two nights after the purchases were made. This was after the police report was filed, the account was closed by the bank, and after the electronics store called her to notify her of the purchase. The lady on the phone representing the credit card company did not even know that the account had been deactivated. She even closed the account again to make sure the first closure went through. This is not comforting to know that the credit card company and bank are not automatically on the same wavelength.

Apparently, the bank had no record of the details of the transactions that took place and neither did the credit card company. They did not have the location of the purchases or whether the purchases were made offline or online. The information was "not available yet."

Apparently if someone you card, without authorization, New York State law requires that you file a statement with the local and state police. After getting everything notarized, signed, and filling out a dozen or more papers, the police kindly took the information. I then asked what should be done about the situation. The police officer behind the desk assured bluntly that nothing would be done since the bank/credit card company had this "sort of thing." I politely asked why we were bothering to fill out a report if the police don't follow up with these types of criminal cases. The police officer said it's up to local police stations whether to follow up with these cases and that most of the cases are taken care of by the credit card/bank companies well before the investigations turn up any results. If an investigation is launched, in addition to filing with local police, you must file with state police who, by the way, are not connected electronically or otherwise with local police stations. Is this not one of the things that caused 9/11 to occur? Have we not figured out yet that law enforcement agencies should be communicating with each other if they are to be effective at stopping crime and major disasters? I am not feeling reassured that we are at all safe in this country.

At this point, you might be wondering why I am writing to your fine publication. Well, this whole thing got me thinking about law enforcement and how utterly useless they can be. Someone steals your credit card and uses it to make illegal purchases, essentially stealing from you, and they can't be bothered to get off their butts and do something about it. Then we all wonder why identity theft and credit card fraud are so pervasive. It's an easy crime and you get away with it too! What kind of message is this sending to would-be crooks? The next

Step is for me to do the research myself. Once I find out where the products were purchased. I am going to try to contact someone at those companies to see if they have any additional information about the purchases. However, I'm not sure how far this will get me as most retailers are nervous about talking to individuals about these things. They become defensive and fearful that you will either expose their insecurities or sue them. Silly rabbits. I just want to know what happened and I think my sister has the right to know this even if the police and the bank are not interested. Sure, the bank will reimburse her \$900 something dollars but that's not the point.

If the credit card companies are going to complain that credit card fraud is rampant yet they do nothing to solve the problem, why aren't they the ones to do something? Ordinary citizens can stop this from going on? Is this some sort of credit card company policy? Think about it. If they can claim that credit card fraud is up there, can they charge you astronomical fees and interest rates and blame it on the criminals. Is this some sort of a ploy to play and account to local/state police to do nothing? Why wouldn't they put pressure on local officials to do their job if this wasn't the case?

Here's where I need your help and your readers help. I would like advice on what to do here. Should I investigate myself by using some social engineering and what tactics would you use to find out more information from those who are not so willing to give it up? Should I write to the local newspapers to find out if they are interested in investigating/reporting incidents like these? Is there anything I am not thinking about or missing here that I can do to stop this sort of thing from happening? Obviously, stop purchasing items online but my sister isn't even sure where the card was stolen. It could have been stolen by someone's cell phone camera in a store or at the checkout counter of the local supermarket for all we know. I need ideas that will help me expose these people for who they are and start a fire under the butts of those who can actually investigate the crime. It annoys me that police are so complicit about this. They should be making examples of these people, not shrugging it off into a lap if they have a hundred thousand dollars a year from fraud because they more than make it up by charging 22 percent interest and 30 late fees. Meanwhile, the rest of us folks have to take days and sometimes months and years to straighten out our credit records and file reports, complaints, and so on.

Any advice on this matter is appreciated.

Adria

You've stumbled into a real nest of corruption here.

The simple fact is that nobody wants to pursue the perpetrators because it's a pain in the ass to prove, almost certainly in another jurisdiction and possibly even in another country, and, most importantly, not cost-effective. As you correctly note, the credit card companies simply pass these charges on to the consumers citing "fraud" even though the money is often taken back from the merchants who then also become victims. These companies lose nothing yet somehow achieve the image of being the good guys because they credit the accounts of the cardholders. Meanwhile, the same lax security that makes such things possible in the first place continues to operate.

You could spend a lot of time tracking down whoever made the fraudulent purchases. We doubt much would come out of that since neither the police nor the credit card company seem all that interested in pursuing it. What would be a lot more worthwhile would be exposing the exact methods used by these people to take advantage of the system. When such a thing is exposed to the world, the companies involved have no choice but to fix them and their failure to do so will finally earn them the wrath they deserve.

Guidelines

Dear 2600:

Can I submit a picture for the back of the zine via email or can that only be done with snail mail?

Brie Stealer

Yes, email is fine. Just be sure it's of decent picture quality. Submit it to articles@2600.com. Payphone photos should go to letters@2600.com. Of course, letters should go to letters@2600.com. Of course, you can also use snail mail for all of these.

Dear 2600:

...be sure to use the highest possible resolution." You really shouldn't tempt 2600 readers like that. The temptation to stretch together a megapixel monster that would make most computers cry for mercy is very high. **Jake**

Let us clarify then. When sending us pictures that you'd like us to consider for printing, you're best off going for something that will look good when it's printed such as 300 dpi. A 70 dpi photo, which is closer to the standard on a web page, simply doesn't cut it in print. Conversely, anything over 300 dpi isn't really necessary.

Dear 2600:

I would like to submit an article for your consideration and would like to know if there is a certain criteria or format that you would like the article in. It does not have any images and just a small script in Perl. All that we like to see is the standard picture formats. Apart from that, we like articles to be as in depth as possible (don't get all preoccupied over length as we can always trim it down) and with a hacker perspective (an air of mischief, lots of what-if scenarios, and a determination not to do things by the book). Finally, we ask that submissions not have been published anywhere else (including websites) and that they not be for two issues after they're submitted.

Dear 2600:

I was wondering what the rules were on article copy-right. When you use an article, are you taking reprint rights? Can the original author use the article in any other form after 2600 prints? Who owns the copyright at that point?

Just considering writing an article, but if it's printed

drive? menu, so Deepfreeze is still bypassable. Of course, the real solution is to stop using removable drives on the affected computers entirely. A central (observed) computer could have removable drives where clients can save and restore work from removable media, and the rest of the workstations could be free of all kinds of removable media.

ManiacDan

The Corporate World

Dear 2600:

I am in an interesting position. I am currently an employee of a McDonald's, the only job I could get in the area at 17. I used to be a computer repair tech with a company in my hometown and I've been hacking my computers, commercial radios, and vintage cell phones for years. In a few days at 10 pm, the McDonald's restaurant where I am currently working will be shut down for system upgrades until around 5 am. All computer systems, routers, network switches, point-of-sale equipment, modems, UPS systems, printers, and racks will be pulled out and replaced with new equipment as the McDonald's Operating Corporation sees fit. I already have an agreement with the store manager and a representative from McDonald's allowing me to collect any equipment I feel I can use or resell.

If you've never been an employee of McDonald's you would be shocked at how the management treats the employees and all the things that go on behind the scenes. Employees are monitored 24/7 with cameras and microphones dangle from the ceiling panels, and I have already written chapters of information on the security system. (I'm not imagining this. Electret condenser microphones are used to record conversations in the restaurant. The McDonald's propaganda posters everywhere in the bowls of the restaurant, the overall Orwellian feel to everything, and you can probably see where I'm going with all this.

I'm going to be bringing home thousands of dollars' worth of computers loaded with proprietary software. I'd just like to get a sense of the interests in an article exposing the entire system. I've already done a write-up on the Internet-accessible surveillance setup that the store managers use to watch us from home.

To keep all of this on the legal side, after the article is written some of the hard drives will be formatted and minimus what I want to keep. Being an amateur radio operator, I have a hobby that takes a lot of money. If I get fired for this, I really don't care. Unlike my sad little managers, I'm actually going to college.

Jon

Our interest in an article like this is of such a magnitude that we doubt expressing our enthusiasm. We will be waiting by the mailbox. (We also took the liberty of removing your last name, call sign, and location from your letter as that most certainly would have gotten you fired. This is one of those rare occasions where we've chosen to err on the side of caution.)

Dear 2600:

I work at IBM and we have had our web activity monitored for as long as I can remember.

I was alerted this morning at work by a coworker that the Firefox and Mozilla browsers (which also means Netscape V7* and V8) support a browser prefetch capability (downloading and caching web pages that you may want to see that's turned on by default).

Also some search engines (Google) do this capability to download pages directly into your web cache as part of the results of a search. The upside to this is that if you do want to look at a link from a search it will show up in your browser faster. The downside is that if the search engine comes up with "questionable" web pages as a result of a search, these can be downloaded to your cache without your knowledge and to anyone monitoring web activity, it looks like you went to the "questionable" web page even though you didn't.

Golden Helix

Dear 2600:

I recently bought an item at Wal-Mart in another state and decided I no longer wanted it. So I returned it at our local Wal-Mart (as they nicely allow us to do). The catch however, is that the tax rates differed between the states by 2.5 percent. When I purchased the item I paid roughly \$63 with 6 percent tax. When I returned it, they calculated the price with the local tax information (8.5 percent) and gave me back roughly \$65. I'm not sure if anyone else had this happen to them, but I found it amusing.

Evil Doings

Dear 2600:

I recently bought a book at Barnes and Noble and would like to comment on the issue around display of 2600 there.

During the four years I worked as a bookseller and cashier I occasionally saw 2600 covered up behind other magazines. This was always in the front row where 2600 was a small, format mag. I never saw it ever be given a policy to hide or not stock or display 2600, but it seems that through carelessness, some customers have covered it up. It is possible that some customers did this deliberately, but I assure the reader that B&N policy is to sell, sell, sell. If they didn't want to sell any mag for any reason, they would not carry it at all, and free up over-crowded shelf space.

I left B&N because I didn't like the new management, so I'm not particularly sympathetic to them, but I see a lot of paranoia regarding this and just want to set it straight.

Thanks for the perspective. We never bought into any theory that such things represented corporate or store policy. But the fact remains that we do have a lot of enemies.

times, some in high places, some in very low places. We appreciate all of our readers being vigilant on such matters and helping to correct any injustices they may come upon.

Dear 2600: I work for a very large telecom whose name I won't divulge for obvious purposes. It all began with the implementation of cameras in our workspace, then with the implementation of "veicept," and now the proverbial straw. I work as a network security analyst monitoring several large networks investigating possible compromises and infections. We all know how the pipe never fits the bib. So they have hired a lot of people I wouldn't have watching over a TI calculator. I get frustrated because nobody has a clue about signatures or even hacker methodology or can even threaten the mindset. So I decided to be a nice guy and put up a bulletin board on my machine at home regarding security, exploits, new code, and several other general categories. Well, the "telecom" caught wind of this and tried to force me to shut it down saying it was a breach of company policy because of the fact I have security bulletin board and it pertains to my job. Where does it say in the Constitution that you give up your rights when you walk into a place of employment? I have sought employment elsewhere and want everyone to know telecons, especially the large and seemingly powerful ones, have no idea what they are doing.

sting3, CEH This kind of thing is unfortunately spreading. There are many corporations and institutions that think they can control their employees. 24 hours a day. Worse, there are so many people who just blindly buy into this, especially if the paycheck is large enough. We need more people like you to keep this from becoming the norm.

NeSurf **Dear 2600:** I have just left my job at Barnes and Noble and would like to comment on the issue around display of 2600 there.

During the four years I worked as a bookseller and cashier I occasionally saw 2600 covered up behind other magazines. This was always in the front row where 2600 was a small, format mag. I never saw it ever be given a policy to hide or not stock or display 2600, but it seems that through carelessness, some customers have covered it up. It is possible that some customers did this deliberately, but I assure the reader that B&N policy is to sell, sell, sell. If they didn't want to sell any mag for any reason, they would not carry it at all, and free up over-crowded shelf space.

I left B&N because I didn't like the new management, so I'm not particularly sympathetic to them, but I see a lot of paranoia regarding this and just want to set it straight.

John Yava **Dear 2600:** It asked for my name, age, major, year of graduation, housing status, and of all things the last five digits of my SSN. Come on... yeah, this is an anonymous survey my ass.... After refusing to complete portions of said survey (portions including questions like: "True or False - hacking is a crime," "Have you engaged in sexual intercourse in the past year?" etc.), I was treated at my dorm room door by the Dean of Students and my RA. Long story short, they were (not openly) threatening me with expulsion. Major WTF moment. I decided to complete the survey and just go along with it but I was sure

Permissions

Plentzios

Dear 2600: While we spend a good amount of time talking about what's going on in the United States, it needs to be made clear that it's getting bad all over the world. Many times our government starts the ball rolling over here and other countries follow suit. But sometimes a new law or restriction starts out somewhere else and winds up later being implemented here. Whenever you happen to be public reaction is essential to influencing the success or failure of such bills and laws. If you can succeed in making a difference, you may also be making a difference in other parts of the world.

Homeland Security

Dear 2600:

BugDave We've followed up with this story on "Off The Hook" and not a good amount of interest from listeners. As it turns out, the local police claimed not to know anything about this and the ensuing fuss apparently resulted in the policy being quietly discontinued. In all likelihood this was something the store was doing on its own. By publicly challenging it and getting people to aware, you helped the store realize that it wasn't in their best interests to continue with such an invasive policy. Individuals have a lot more power than they realize.

Dear 2600:

The other day, for the fun of it, I thought that I would see if the full version of *Delta Force - Black Hawk Down* was available for download on Limewire (a P2P file sharing program on Gnutella). When I typed "Delta Force" in the "programs" search window and clicked "submite" hundreds of files popped up claiming to be "Delta Force Full Game" (but were only 851.7kb in size obviously too small to be the actual program). These files were all uniformly the exact same size although they were all being "shared" by several different users. When I typed in "Grand Theft Auto" the exact same thing happened. Several files claiming to be "Grand Theft Auto" were also 851.7kb in size and from multiple users as well. It appears to be an attack on P2P file sharing in general, but surprisingly, several people seem to be on it. As we all know, 851.7kb is definitely more than big enough to be a trojan horse, virus, or worm. Does anyone know what this file is or who is responsible for this?

Dear 2600:

Two days ago I was sitting in my Atlanta-area high school's computer lab and decided to check the news at 2600. To my dismay, it was blocked by the school's administrator. However, what really irked me was the fact that it was labeled under the category "Criminal Skills." I was most definitely not expecting this level of ignorance from the school, but I guess in today's society that was a little stupid of me.

Ben

Schools are where ignorance is taught and reinforced. What were you thinking? For that matter, why were you thinking? I will try to be brief. I bought some beer over the weekend at Western Michigan University at a store called Munchie Mart. They asked to see some ID and I showed them. After giving them my identification they then

swiped it through a mag strip reader that had a built in printer and tape roll (looked like a printing calculator). I noticed it printed my name, age, and driver's license number. After noticing this I asked the lady to hand me the copy of my personal information so I could discard it. She refused and told me she had to record it for the city police in case they sell to minors. I was outraged! I started to argue some more and then was told "if you have a problem with it, then don't shop here." I told her I would as I was only visiting a friend at the university with this. I know it's only minimal information but that's not the point at all. I am also considering writing to the Kalamazoo police inquiring if they enforce the unauthorized recording of personal information. I wonder how many identities they sell to minors?

Taot-sama Don't be shy about revealing the name of the school. You can also get an extra copy of the survey (somewhat) and send one of those in. Nothing defeats this kind of bullshit quicker than a little publicity. Hang in there.

Dear 2600:

I thought you guys might be interested in a reminder that September 24th started Banned Books Week, my favorite holiday and a celebration of the right to read despite the best efforts of small minded zealots everywhere. It's continually amazing to me that many people would work so hard to suppress, repress, and oppress anything that threatens their safe little cocoon of "decency" and political correctness rather than dare to expose their children to different or unorthodox ideas which might spark a debate.

Check out the Top 100 Most Frequently Challenged Books of 1990 - 2000 (from <http://www.ala.org>): This endangered species list includes classic literature such as *The Adventures of Huckleberry Finn* (#5), *Catcher in the Rye* (#13), and *To Kill a Mockingbird* (#41). Worse yet, it is peppered with perfectly innocent children's books like the *Harry Potter* series (#7) and *Where the Waldo* (#88) which I don't believe even has any words. And no list of dangerous books would be complete without *The Anarchist's Cookbook* (#57).

Whether it's during or after Banned Books Week, please remember to celebrate the glorious fight to read books that challenge the established norm, shake up stereotypes, and present old situations from new points of view.

"Books won't burn. Ideas won't go to jail. In the long run of history the censor and the inquisitor have always lost. The only sure weapon against bad ideas is better ideas." - Alfred Whitney Griswold (Yale President 1951-1953)

Information is still free. Read a banned book - or better yet, write one!

Selena

Dear 2600: The exact same thing happened. Several files claiming to be "Grand Theft Auto" were also 851.7kb in size and from multiple users as well. It appears to be an attack on P2P file sharing in general, but surprisingly, several people seem to be on it. As we all know, 851.7kb is definitely more than big enough to be a trojan horse, virus, or worm. Does anyone know what this file is or who is responsible for this?

Ben

Schools are where ignorance is taught and reinforced. What were you thinking? For that matter, why were you thinking? I will try to be brief. I bought some beer over the weekend at Western Michigan University at a store called Munchie Mart. They asked to see some ID and I showed them. After giving them my identification they then

bus/chamblis/house/bills/government/C-74-1.PDF if you'd like to take a gander. Keep fighting the good fight.

Plentzios

Dear 2600: While we spend a good amount of time talking about what's going on in the United States, it needs to be made clear that it's getting bad all over the world. Many times our government starts the ball rolling over here and other countries follow suit. But sometimes a new law or restriction starts out somewhere else and winds up later being implemented here. Whenever you happen to be public reaction is essential to influencing the success or failure of such bills and laws. If you can succeed in making a difference, you may also be making a difference in other parts of the world.

Dear 2600:

Elegin I would like to get permission to show The Fifth HOPE videos at a Linux user group meeting. There are about 20 attendees on a good month.

Uncle Wulf

You're more than welcome to do this. We've had some people even manage to get a few of these onto public access channels on cable television. We'd glad to see videos at this and other conferences we've hosted. It's also great for those people who weren't able to make it in person.

Dear 2600:

Elegin I'm in a community college web programming class and we're working with javascript at the moment. Would you mind I copy Edward Stoever's article "Hacking Encrypted HTML" from 22:2 for distribution to my less enlightened classmates?

Uncle Wulf

We encourage this kind of thing as long as you're not selling it and you give attribution.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin We're glad you were able to deal with this maturely and non-hysterically. If only this were the rule and not the exception.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I discovered about a year ago that Northwestern University has automated book checkout stations on many of their floors. You can scan the barcode on your library card, the "WidcatID" (university ID card) usually, enter your last name into the computer, and then scan the barcode for making us aware of the problem.

Dear 2600: We're glad you were able to deal with this maturely and non-hysterically. If only this were the rule and not the exception.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to GID4P for making us aware of the problem.

Dear 2600:

Elegin I used to subscribe back in 96/97. A car forum I'm a user on got hacked by the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The

their trash methods. You could easily get the trash can full of book receipts from one of the sleepy college kids working at the circulation desk, honest account info, make fake cards, and congraduate the other sleepy cod in the book but doesn't check that there's a slip in the book.

If Northwestern does this and claims to be the tenth largest private university library in the country, then I imagine other college libraries are doing similarly. Inse-
cure things with their book receipts and self checkout.

Nick B.

Offenses

Dear 2600:

Yesterday, I frequented Barnes and Noble and picked up a copy of your magazine. I went and grabbed a coffee and sat down and started to read. I got to the section on readers letters and happened to read one from someone who was upset because of the way you had associated Taiwan with the Republic of China. This didn't upset me too much. I thought it was just a case of political correctness. But when I saw on the back page a phone in Syria with the words "Arts of Evil" I was extremely upset. I thought your magazine was wise to the world as political parties. Obviously your magazine is a lot more closed minded than I thought.

Short

Yeah, you got us. We tend to blindly follow what our government tells us so when we heard that there was an Arts of Evil we naturally believed it without question. It is now our understanding that they don't actually call themselves straight. Oh and for the record, Taiwan and the Republic of China are the same place. But the last thing we want to do is start talking about that again.

Dear 2600:

I am very disappointed by your response to Hsiao-Ling Liao (222). What happened to your rhetoric? ... we have a history of not blindly accepting what we're told" (page 5, line 12, 2014). Do you believe that ISO 3166-1 has "Taiwan, province of China" for scientific reasons? I can assure you that it is from political pressure from the Chinese government. Isn't it ironic that we hackers use extra effort to filter what the U.S. government tells us, but take in what the government of China says without thinking?

Yes, we Taiwanese, fighting against China's imperialism (they claim to be socialism but believe more like imperialism), understand that ISO 3166-1 is the source of misinformation and we are fighting on that front too. Taiwan is not so stupid as to call itself a province of another country.

You are fully responsible for the content on your website, even though you are not exactly responsible for how Taiwan is officially designated. I checked it just now (<http://www.2600.com/phones/mewindex.khtml?region=asia>) and you are still using that insulting suffix despite your lip service in 222.

Google: they removed the insulting suffix when facing massive protests from Taiwanese netizens but reverted after pressure from the Chinese government who threatened to block Google from the search engine market in

China. Sadly, Google is not the only one. Many U.S. corporations do the same when facing threats from China. We all knew it was inevitable that 2600 would wind up in the middle of this conflict. But let's get a few things straight from the outset. We are not referring to Taiwan as "Taiwan, province of China." We are merely accessing an official list of countries and that list happens to be worded in this manner. The mere fact that Taiwan is represented at all on the list has annoyed mainland China, so it's a bit of a two-edged sword. It would solve nothing if we went in and changed our copy of the list and it would open us up to having to change all of the other names that people have a problem with. Then there would be people who have a problem with us changing the list. We would then be condemned in the world of international conflict where we wouldn't stand a chance of addressing those issues that really matter to us like fixing the definition of the word "hacker". The solution to this forum helps achieve that and then we're happy to be of service.

Tim Taiwanese Littm
New Jersey

We all knew it was inevitable that 2600 would wind up in the middle of this conflict. But let's get a few things straight from the outset. We are not referring to Taiwan as "Taiwan, province of China." We are merely accessing an official list of countries and that list happens to be worded in this manner. The mere fact that Taiwan is represented at all on the list has annoyed mainland China, so it's a bit of a two-edged sword. It would solve nothing if we went in and changed our copy of the list and it would open us up to having to change all of the other names that people have a problem with. Then there would be people who have a problem with us changing the list. We would then be condemned in the world of international conflict where we wouldn't stand a chance of addressing those issues that really matter to us like fixing the definition of the word "hacker". The solution to this forum helps achieve that and then we're happy to be of service.

Chad

There are those in Taiwan, incidentally, who believe that mainland China will eventually be reunited under the Taiwanese flag. They consider all of the provinces of mainland China to belong to the Taiwanese regime. That, coupled with the fact that Taiwan calls itself the Republic of China, gives a much more positive spin to the whole "Province of China" moniker. It all depends on how you define China. But seriously, the one sure way to solve this problem is, rather than start a fight with us, to declare independence from the mainland. It may take a civil war and several million lives but ISO 3166-1 will be changed.

Dear 2600:

I really enjoy your mag. Whenever I go to the States I pick it up. I don't normally write to a mag. But something I read recently made me mad. I read 222 today and I was pissed. Answer this question. What do you stand for? Does "Free Kevin" mean anything to you? Do you see where I am going with this? 2600 are the biggest hypocrites on the face of the earth. I read your message that now to attend any 2600 meeting you need to dress how did you all put it. In standard formal attire. Wow, this goes against everything you fight for. These meetings are, for a lack of better words, "for fun," to gain knowledge from fellow administrators (hacker). It's not a business. It is not church. It's not a Fortune 500 company. We as administrators live in a culture that we can wear whatever we want. I work at an IT company and attend many meetings. My dress is not standard for attire. You state that "nobody is excluded" if they comply with the guidelines. They are guidelines, not rules. And until you pay me the money that comes with wearing standard formal attire I shall wear whatever I want to any 2600 meeting because "nobody is excluded." I think

you are doing just what you are trying to fight. I will continue to read your fine mag for the tech articles but not for what you stand for.

Ramasse

It's pretty obvious we're going to be getting this kind of letter for years to come from people who don't understand the concept of April 1st in the United States. Considering we even alluded to it in the issue you cite, we don't really know what else we can do. Humor really can be a dangerous implement.

Dear 2600:

First of all, let me tell you how much I love your magazine. It's been a great joy of mine for a long time now. Also, I don't have a subscription because not only do I not have the money for the stand price. Now, a while back I decided to go to the 2600 meeting closest to me (Michigan) and wanted assurance others would do the same. I opened up one's there. I promptly joined #2600, expecting knowledge abounding. Instead, I was met with the most rude and mean-spirited attitude I've ever seen. I informed myself in a very polite manner and was met with a person telling me to "shut the f*** up or go away." Naturally, I was befuddled as to why they would tell me such a thing. I replied with mildly sarcastic comments and was met by more anger and insults. I realize the world is a cruel place. I have grown up in a bad part of town. Despite my efforts of trying to learn all I can, I'm met with hate everywhere I go. I thought you valued the exchange of information and the pursuit of knowledge. Shame on you.

Shane

Shame on us? Oh, please. You can't possibly expect an RC channel to represent anything other than a group of people sporting forth whatever is on their minds. Sure, we like to have intelligent people in the #2600 channel on irc.2600.net since it's our flagship channel. But it's impossible, and undesirable - constantly monitor, and control the flow of conversation. That means that idiots and assholes appear from time to time and attempt to get attention by being offensive, loud or just plain stupid. It happens. They are actually less annoying than people who take it so seriously. You have to learn to weed out the morons and listen to those individuals who actually have something to say. They exist in great numbers, but please remember that it's just a gathering of people who decided to join an open channel. Occasionally, there may be a 2600 staff member or writer in the channel as well, but we're often busy dealing with other more urgent matters. So get back in there and make the channel a better place rather than issuing condemnations and slinging away while muttering to yourself. You'll feel better.

Dear 2600:

I really enjoy your mag. Whenever I go to the States I pick it up. I don't normally write to a mag. But something I read recently made me mad. I read 222 today and I was pissed. Answer this question. What do you stand for? Does "Free Kevin" mean anything to you? Do you see where I am going with this? 2600 are the biggest hypocrites on the face of the earth. I read your message that now to attend any 2600 meeting you need to dress how did you all put it. In standard formal attire. Wow, this goes against everything you fight for. These meetings are, for a lack of better words, "for fun," to gain knowledge from fellow administrators (hacker). It's not a business. It is not church. It's not a Fortune 500 company. We as administrators live in a culture that we can wear whatever we want. I work at an IT company and attend many meetings. My dress is not standard for attire. You state that "nobody is excluded" if they comply with the guidelines. They are guidelines, not rules. And until you pay me the money that comes with wearing standard formal attire I shall wear whatever I want to any 2600 meeting because "nobody is excluded."

Dear 2600:

I am from New Zealand. Until recently I have been working for Restaurante Green Party Member of Parliament Nandor Tanczos. One of his portfolios was IT and I was his advisor. I am an avid reader of your magazine not just because it is exceptionally interesting but also because it was a source of support for something trying to push the lines within "the institution." Anyway, the *National Business Review*, our right wing as fuck newspaper, just wrote a big article slagging the Green Party off for their support of OSS and I got dragged back in to help write a response. 2600 got mention so I thought to let you know and take the opportunity to thank you for all the support you gave me over the last three years. Who knows, I may even have time to write an article for you about institutional activism!

Dear 2600:

I am from New Zealand. Until recently I have been working for Restaurante Green Party Member of Parliament Nandor Tanczos. One of his portfolios was IT and I was his advisor. I am an avid reader of your magazine not just because it is exceptionally interesting but also because it was a source of support for something trying to push the lines within "the institution." Anyway, the *National Business Review*, our right wing as fuck newspaper, just wrote a big article slagging the Green Party off for their support of OSS and I got dragged back in to help write a response. 2600 got mention so I thought to let you know and take the opportunity to thank you for all the support you gave me over the last three years. Who knows, I may even have time to write an article for you about institutional activism!

Dear 2600:

I am always welcome articles from those who are somehow inside that system. It's good to know our words have managed to penetrate from so far away.

Discovery

If you're feeling a little bored, go to Google, type in "Failure" then click on "I'm Feeling Lucky." I'm glad to describe and link to President Bush's website, thus pushing it to the top of searches for those phrases. If you click on "Google Search" instead of "I'm Feeling Lucky" you'll see a link to the full explanation on the right hand side of the page. As an exercise, let's all see if we can make the word "maniac" go to <http://www.whitehouse.gov/vicepresident/vpbio.html>.

On The Inside

Dear 2600:

I really enjoyed Xlogix's article about manipulating the call center systems in 223. I thought I'd share one of

Personnel and Social Engineering

by subpreeky

subpreeky@yahoo.com
Social psychology is essentially the branch of psychology that studies the behavior of individuals as they interact. This is not the same as sociology, which is essentially the study of human behavior in groups. Social psychology can be especially interesting when relating to social engineering, as much of the study of social psychology deals with *why* and *how* humans are able to influence one another, both as individuals and as groups.

Elements of persuasive communication fall into three main categories: the characteristics of the speaker, of the message, and of the listener(s). Of the characteristics of the speaker, *credibility* is one of the more important persuasive factors. The speaker must be a credible source of information to be persuasive. Although speakers with low credibility will be less persuasive at first, they can often influence thinking and behaviors over a longer period of time through a phenomenon called *sleeper effects* (this can be close to a persistent nagging type influence). Speakers are generally more persuasive when they are physically present with an audience. This may present obvious difficulties when attempting to social engineer an audience over the telephone and/or the Internet. The speaker's intent is also important. If an individual is obviously trying to change an opinion or behavior, the speaker will be less persuasive. Care must be taken by the speaker so that the listener(s) do not feel that they are being taken advantage of in any way. Humans have a natural desire (although not always a tendency) to trust other humans. If trust is broken by the speaker in any way, the speaker will be less persuasive. In general, authority figures can be persuasive to a degree (perhaps our president can be considered an exception).

First impressions of the speaker are *very* important to the listener(s). First impressions are also known as the *primacy effect*. The primary effect will be different from listener to listener, as two people will perceive the same person differently, mainly because of differences in interpreting the individual's traits. Attractiveness can be important for the speaker, especially as the first impression is weighed by the listener. In the end,

however, physical attractiveness of the speaker generally only determines persuasiveness when dealing with relatively minor issues. It should be important to remember that when a first impression is made by the speaker, negative information is generally weighed more than positive information in person perception.

The second element of persuasiveness is the message. This is probably the element of persuasive communication that the speaker has the most control of when social engineering. Emotional appeals and two-sided arguments are the two main characteristics of the message that determine persuasiveness. Of emotional appeals, fear tends to be the most persuasive emotional trait of a message. However, the listener(s) typically only respond favorably to fear if (1) emotional appeal is strong; (2) the listener(s) believe that the fearful outcome is likely to happen to them; and (3) the message, or outcome of the message, offers a way to avoid the fearful outcome. Regarding two-sided arguments, when communicating to an audience that initially agrees with the speaker's position, the speaker will generally be more persuasive if both sides of the argument are *not* presented. However, when communicating to an audience that is initially unfavorable to the speaker's position, both sides of the argument should be presented. As an interesting note, logic is not necessarily an important factor in determining a message's persuasiveness.

The third element of persuasive communication, and the element that the speaker has the least control over, is the listener(s). In general, less intelligent people will be easier to persuade. On the other hand, if the message is more complex, more intelligent listeners are easier to persuade. Also, people with a need for social approval and/or low self esteem are often easier to persuade. An important factor of the listener(s) that the speaker may have some control over is that people are easier to persuade when listening to a message in a group. Larger groups are easier to persuade than smaller groups. The main reason for this is conformity.

Remember, social engineering is something that can be learned and used overnight. Much practice and experience is needed to become a skilled social engineer. Remember, too

- that not everyone is meant to be a skilled social engineer. A few helpful tips:
 - Have your entire message planned out. The more detailed your message is, obviously the more believable it will be. If necessary, write down what you want to communicate on paper, and allow much room for hypothetical situations.
 - If you are with a group of friends, pick out the person that has smooth social and communication skills, is a fluid speaker, and/or someone whose appearance is not too far out of line with the social norm (for example, the friend with a three foot purple and green mohawk and facial piercings will be less persuasive in person
- Understand all of the elements that come into play with the communications medium that you are using. Think beforehand about what and how you want to say something in relation to being on the telephone, in person, on the Internet, etc.
- First impressions are very important when trying to social engineer an audience.
- Remember, the art of social engineering is just that - an art.

The Real Electronic Brain Implantation Enhancement

by Shawn Frederick

waxcast@juno.com

I am not a medical doctor, nor does my background in science reflect much neurology. I am however a scientist, and currently work for two different laboratories. This article will offer insight on the factual and idealistic concept of electronic implants working for or alongside the biological nervous system and brain of man. To keep the attention of my audience I will do this with as minimal biological workings (no more than high school biology) as possible. The theories are my own.

Computers only rely on the laws of Boolean mathematics while the biological makeup of man's brain follows the laws of physics. There are more chemicals in the human brain that modern medicine does not understand or know of than there are those which are understood. These chemicals can be responsible for such things as anger, happiness, and even thirst; they also are responsible for invoking long and short-term memory. The human brain is extremely complex, but what if we were broken down into a more simplistic system that resembled computer functionality? Whereas science has a grasp on how the brain essentially works, we are still in the dark as far as understanding human consciousness. For example: 2+2=4. Yes, a computer can tell you this and yes, it reacts a certain way based on an answered value. For humans however it's more than just Boolean. How does one understand and manipulate the meaning of a number or creatively envision and paint a picture? This article is not asking the age-old question "what does it all mean" but merely acknowledging that in all its obviousness human awareness will play a large role in the times of brain implantation.

There are a few different theories on how the brain's memory (database) works. For the purposes of a short article we will focus on the more popular theories. Short-term memory is

described as the mind holding a thought via an electrical circuit. As long as the circuit is continually used the memory can be held. If it is continuously stimulated the short-term memory may then transition to permanent memory where the human brain physically changes its shape. It is believed that the brain stores information on the cellular level. With all the different theories there are about how the brain actually works, the truth is that no one knows for sure how it really functions. Medicine has a general idea of the mind's mysterious mechanics, but still is closer to uniting quantum physics with Einstein's classic physics (this is a joke).

The Browser Offers Info

to Human Awareness (A)

Whereas science has a grasp on how the brain essentially works, we are still in the dark as far as understanding human consciousness. For example: 2+2=4. Yes, a computer can tell you this and yes, it reacts a certain way based on an answered value. For humans however it's more than just Boolean. How does one understand and manipulate the meaning of a number or creatively envision and paint a picture? This article is not asking the age-old question "what does it all mean" but merely acknowledging that in all its obviousness human awareness will play a large role in the times of brain implantation.

There are a few different theories on how the brain's memory (database) works. For the purposes of a short article we will focus on the more popular theories. Short-term memory is

Winter 2005 - 2006

mentation found, offers it up to the human consciousness (AI). Humans are still very primitive; some are running Internet Explorer and Netscape while others are using Firefox or Lynx. The truth of the matter is that from the most superior genuses at NASA to the mentally impaired, the difference is almost none when looking at the vast picture. Kim Peek is a prime example of this.

At this moment and time it's impossible to scientifically explain human awareness, but some refer to it as the soul. It is linked to creativity and free will. Human awareness is only as good as the "database" and "browser" one has.

The analogy of quantum physics meets Einstein's classic physics was used once already in this article and seems fitting to use again talking about the "browser" of the human brain offering information up to human awareness. There are a few good theories on the medical explanation of human awareness, but I recommend Francis Crick's *Astonishing Hypothesis: The Scientific Search for the Soul* if interested.

Humans Interact with the Mattered Universe

The most advanced brain-driven mechanical instruments we have are a few robots and electroencephalogram machines. I also have read that the military has VR that imprints images directly on ones retina (different subject). As cool as the brain-driven robots and EEG machines are, these technologies have little room for advancement and are really no better than a mood ring. The technology reacts to human electrical stimulation. What is really needed is to be able to think a thought on a number and have it appear on a computer screen, enhancing one's intellect with physically jacking into or wirelessly jumping onto the Internet. Unfortunately the "code" of the human mind must be cracked before we can truly see any brain implants or VR worth obtaining.

How I Believe It Will Come To Pass

How do we as humans feel the soft touch of a woman or interact with the surrounding world of matter that we live in? In order to react and comprehend the matter of the universe, we have electrical impulses and chemicals that flood our brain at any given time. But broken down it looks like this.

Peripheral Nervous System

Brain

The peripheral nervous system connects the CNS and the brain. Their working together is the only way humans understand textures of the world in which we live. When programming a computer one feels the keys because a chemical is released, read by receptors, and electrical impulses passed from node to node to the spinal cord. The message is then sent and encoded just

before or in the brain. I use the word encoded because the spinal cord doesn't tell the brain that the PHS is feeling a rough or coarse textured surface. From my understanding it is all sent via an electronic biochemical reaction that travels module to module, on the axons. The message must be coded until the brain gets the info and can explain or "decode" what is electronically being sent. I will add to this that the electrical mode of transmitted information is actually biochemical. The electrical impulses (the jumping from node to node) are stable until reacted upon. An impulse is produced chemically from an inverse reaction of naturally charged atoms of Potassium (K) and Magnesium (Mg), which are cat ions (positive charged) with a few anions (negatively charged) Chloride (Cl) and bicarbonate (HCO₃⁻). The electrical charge is significant to the audience of this article.

Brain + human awareness = nervous + muscular and skeletal system = action upon matter. Anything else reacted upon or observed in our universe is photonic (nothing more than light photons bouncing off matter) or sound waves (matter is only understood to the brain when it's told electronically). Human awareness, soul, AI consciousness, whatever you will call it is needed for understanding the processed/decoded information - that a picture on the wall is a picture and not just a bunch of bouncing photons.

The Day of Brain Implantation

If humanity does not destroy itself first there will be a day that electronic implantation will be as natural as human sexuality. But the most brilliant of hackers couldn't develop an implant with the great potentials that have been discussed. A programmed implant interacting simultaneously with the nervous system and mind would be a sure fate, done by a team of doctors, research scientists, and programmers. When brain implants come to pass they will need to be implanted where the spinal cord meets the brain (foramen magnum). This is believed to be true based on knowledge that information is electronically sent and possibly interpreted in that general area.

Obviously any implant created could not be plug and play. Every individual is unique in the way his or her brain works, both biochemically and electrically. The future implant will not only have to sometimes, share, or piggyback off the electrical impulses that are being sent via the spinal cord. It would either have to manipulate the spinal cord or use it analogically like a USB 2 cord. The future may allow advancement to bypass the spinal cord completely, sending its electrical messages directly to the "decoder" (possibly thymus) of the brain, then on to the "browser." The implant would need to do this

wearing it which should do away with watches).

Problems With Brain Implants

As most testing goes, it will start out in a laboratory on some animal, more than likely chimps. It's scary because we are a primitive species. There is no doubt that no sooner will we discover how to create such a device than someone will use it for the worst possible thing imaginable. It will be advertised as a harmless, monitored environment. But how can anyone be sure that he or she isn't being used or manipulated? Evolution is responsible for enhancing man's mind and controlling it chemically and electronically. Implants will be commonly used unfortunately. There will be no need for memory or for us to use our biochemical minds as nature intended. The human species will have taken the role of half biological half robotic while our brains evolve to much, totally useless, and completely reliant on implants.

I hope it doesn't happen like this. But in addition, there is the prospect of genetic enhancements in mankind's evolutionary future. That is a whole different article but offers the same wonders and terrors.

Was it really worth what you had to go through to get your hands on this issue?

Did you have to drive a huge distance or take a long ride on mass transit to get to the only place around that had it in stock? Did you lose a friend by furiously fighting over the last copy? Or is it maybe driving you crazy knowing that each issue you buy at a store costs a few pennies extra than if you had it sent right to your home/office/prison? Doesn't subscribing seem like a good idea? Of course it does!

There are two easy ways to subscribe. You can go to our online store (store.2600.com) and use your credit card. Or you can send \$20 (U.S.) to 2600, P.O. Box 752, Middle Island, NY 11953. If you're overseas, make that \$30 and add "USA" to the address.

What's this? You're still not sure? Perhaps the fact that only subscribers can place free classified ads in our Marketplace section will finally make you see reason. Yeah, we thought so.

ing from the pattern. Rob made a note of this. It was also about this time that he started keeping track of the winning numbers to see if there was a pattern. After a while he discovered that the first number in the first row came up quite often - almost 50 percent of the time. Because of the way the machine was designed, when they released the balls, this first ball must have fallen directly into the area where the balls were drawn

By Leeday I have a friend (I'll call him Rob) who supplements his regular income with money made from the lottery. He does this in two ways - he publishes newsletters which contain tips and "hot" numbers, and he is a long-term net winner in playing the lottery himself. He does this by tracking the winning numbers and coming up with a "hot" list - numbers that are coming up more frequently than others. As anyone with any mathematical aptitude for math or odds certainly knows, this is a link, as you cannot predict future random outcomes by looking at past results. But as anyone with any sense can figure out, ping pong balls are not manufactured with great precision. There are slight variations in weight and shape, along with minor imperfections. How these differences in lead to predictable patterns is well documented in several books that tell of roulette games in Las Vegas that were not manufactured with precise tolerances and the MIT students who were able to win large amounts of money each summer to finance their education. To understand this, first, consider the following:

on a single number, you will bet you can expect to earn back only 35, or about \$945 for every \$1000 wagered. The lottery works a little differently - it is a multi-part/multi pool where a certain amount is set aside for paying off winning numbers and the payout for any particular number depends on how many people selected that number. Many lottery players try to determine which numbers no one else likes and play those instead of playing their "hot" numbers. Regardless, the typical payout for a Pick-3 lottery is \$200-\$300. With three digits there are 1000 numbers so the odds are 1000 to 1 against you. For every \$1000 you wager in a Pick-3 lottery you can expect a return of \$200-\$300 back - certainly much worse than Vegas. With those odds against you, it is easy to see why a little numeric edge in selecting numbers has not allowed Rob to take an early retirement.

But that is not the hack. The hack was far simpler than that and is how Rob got started writing and selling lottery newsletters. Rob has been an avid lottery fan for over 10 years. He has

After my education, I worked on insulation a few years ago when I used to volunteer work for a local civic organization, working at their nightly bingo games. We had two sets of bingo balls that I would rotate every so often. One set apparently had a few balls that were markedly different from the other balls and, as a result, would draw much less frequently than the other balls. It was noticeable enough that the old ladies who played every night would complain to us after every few or four days to switch the balls. They were not allowed to hand pick their own cards, and the more astute ones would search for cards without the dead numbers on them, just in case.

by Stepanovich I was recently hired at Sears Portrait Studio have any number of excuses should they be caught. On the front desk there are at least two

and discovered some disturbing issues during my training. Their knowledge of basic security measures is tenuous at best, and they seem to regard customer privacy as little more than a nuisance. First, you must understand the basic layout at SPS (their internal name). The front desk is typically free floating and customers could very easily get behind it without being seen. They would computers, more for bigger stores. There will be at least one standard terminal (all of them are Dell) and a POS terminal which is IBM. These are identical to the other POS terminals used in Sears. All of the desktops are running Windows XP Professional and I believe the IBM runs DOS. However, the only program they seem capable of running is the sales kiosk.

Observing the Lottery

By Lesley I have a friend (I'll call him Rob) who supplements his regular income with money made from the lottery. He does this in two ways - he publishes a newsletter which contains tips and "hot" numbers, and he is a long-term net winner in buying the lottery himself. He does this by tracking the winning numbers and coming up with a "hot" list - numbers that are coming up more frequently than others. As anyone with any knowledge of probability for math or odds certainly knows, this is a link, as you cannot predict future random outcomes by looking at past results. But as anyone with any sense can figure out, ping pong balls are not manufactured with great precision. There are slight variations in weight and shape, along with minor imperfections. How these differences in lead to predictable patterns is well documented in several books that tell of roulette needs in Las Vegas that were not manufactured with precise tolerances and the MIT students who made yearly pilgrimages each summer to finance their educations. I witnessed this firsthand a few years ago when I used to do volunteer work for a charitable organization, working at their nightly bingo games. We had two sets of bingo balls that I would rotate every so often. One set apparently had a few balls that were markedly different in weight from the other balls and, as a result, would be drawn much less frequently than the other balls. There was noticeable enough that the old ladies who played every night would complain to us after a few hours or four days to switch the balls. They were not allowed to hand pick their own cards, and the more astute ones would search for cards without the "hot" numbers on them, just in case

were using that set of balls that night. Anyway, a round 12 years ago, Rob commissioned me to write a simple tracking program so could load the winning number history for any year and let the user determine not only the "hot" numbers, but hot sets of numbers (for example, if two or more numbers are likely to be drawn together). The lottery has a huge odds advantage in that the payoff ratio is far lower than a actual odds. This is the "house edge" that always works them to make money. To give some perspective, most roulette wheels in Vegas have 37 numbers (1-35, 0, and 00) and pay off 35 to one.

There is typically a dividing wall behind the desk but it doesn't extend fully to the sides. In front of the wall is a row of cabinets (not locked) which contain records of all kinds, photos to be picked up, and so on. On top of the cabinets are assorted papers being used and the in-store printer. It wouldn't take much imagination to grab photos from this, since they're typically left sitting in the tray for some time before being sorted. Connected to the printer is another desktop running Windows Server 2003. I'm not sure what its function is, other than it allows for full control of all images, print jobs, and customer databases. It also has remote access capability, since during a technical support call they were accessing it.

Behind the wall are the viewing stations. This is where customers are taken after a shoot to decide which packages, sheets, and any enhancements (black and white, sepia, duotone, etc.) they want. They are nothing more than another desktop with SPS software that allows image review, basic manipulation, printing, ordering from the lab, and many other functions.

Finally, in each studio there is another desktop which is connected directly to the camera and also has SPS software installed. Typically after a shoot, the photographer will do some basic manipulation on a few of the images, such as black and white or vignetting, which will then show the customer at the viewing stations.

Now the interesting thing about the viewing stations is that they all have full access to the image database which contains every photo purchased for the past six months. They also have separate accounts set up under Windows, with user names such as sales, studio, and admin. The passwords, sadly, are the same as the user name. Even worse, every associate knows this and is often seen repeating them out loud in front of customers while typing them in. (Some functions are disabled except to the administrator and so it is needed from time to time.) From here, malicious person could wipe out their entire image collection or insert their own. In theory, one could replace images in the print queue with one's own and then grab them from the printer before they were noticed.

The desktop at the front desk is the main terminal, which has access to the customer database and the appointments book. All of this is done through a web interface to the main SPS website. It uses standard 128 bit SSL with the client running IE6. This is probably the biggest security hole in the entire operation. The website is typically left up, to avoid having to open it back up every few minutes. From here you can view, modify, and add appointments, look up cus-

tomer information, view sales figures, and most importantly, clock in and out. Note however that none of the desktops, including the front desk, have full Internet capability. The only website allowable is the previously mentioned web interface. Whether this is locally implemented or via a separate firewall is unknown.

Now the employee clock deserves a bit of background information. Every SPS employee is issued a three digit associate number. It doesn't seem to follow any sort of pattern and they actually are guarded fairly well. This number, however, is not required to perform any of the above activities. It is only used for initial login of the kiosk but, as I mentioned, it's usually left logged in. To clock in and out you use your social security number which pulls up your information. After verifying it is correct, you are clocked in. The store manager has a unique ability, however. They are able to modify the clock times. So for instance if an employee forgets to click in upon arrival, it can be modified to show that they did. The manager account has a few safeguards in place. First, you must know the store's ID number. This is easily obtained either by glancing at the screen or through a small bit of social engineering. I imagine registering a complaint would be a valid excuse to obtain the number. Second, you must know the manager's associate number and the last four digits of the social security number. They are used together as a password of sorts. As I mentioned, the associate numbers are fairly well guarded so you would have to hope for them to be pasted to the screen or some such. In all honesty, that wouldn't be very far fetched.

Above all, of course, you could try brute forcing it but trying 900 combinations by hand isn't very feasible. As to the social security number, that would be a bigger challenge. The last four digits scheme is used by several companies now, including banks and travel agencies. It would be possible, therefore, to do a bit of social engineering with them, provided you had sufficient information.

My biggest concern overall are the viewing stations. They are completely at risk and not protected in the slightest. The photos they contain are the property of SPS. It would be a significant financial loss if someone were to download them to a flash drive or similar, rather than pay the exorbitant fees (\$80 currently) to buy the rights to them. Worse yet, imagine an individual obtaining customer information, as well as a decent amount of photos, and then selling them at reduced prices to the clients. This would be completely undetectable as there are no logs or other safeguards in place.

Unfortunately it was turned off and pushing the power button did nothing. It must have been unplugged. But then I noticed a little binder on the top of the machine that had a cover saying "Kodak Picture Maker 63" so naturally I was wondering what this was. I picked it up and looked through it. It actually had the manual for this machine! And on top of that, it had three CDs in little pouches. They were labeled "Kodak Picture Maker shortened to KPM" "KPM - Training tutorial V2.0," "KPM - Wal-Mart Special 1 - 63 Software," and "KPM - Application Software V3.7 SP1 (Full Install)."

This

is when I flipped. I had access to the

software on these things. I really wanted this

software but I didn't want to steal these things.

So I came up with this plan: I would come back at

2 am. I chose that time because I would be up

Kodak Secrets and Wal-Mart Fun

by Thorn

thorn2600@yahoo.com

This is really two articles in one: a true story of a crazy adventure getting software and showing some flaws in Wal-Mart's security, as well as an article on the software and manual I obtained from that adventure, the Kodak Picture Maker 63. If you are unfamiliar with what that is, it's the big Kodak machine in stores like Wal-Mart that you use to scan pictures. You can also use pictures on whatever type of disk you might have and edit them, change the size, make more prints, or whatever.

Now obviously I'm not going to put the entire manual in this article... I plan on eventually ebooking the whole thing and putting it online, but I'll just give you the juicer parts for now such as how to change settings, retrieve "lost" passwords and/or change passwords; as well as the stuff they don't want you to know about this software. But first I will tell you all a story of how I obtained this material because it is one crazy story which also points out Wal-Mart's insecurities.

A friend and I were at Wal-Mart and we went to the usual department we liked to look around in: electronics. Next to it was the photo department and I started messing around on those self service machines with the scanner, the monitors, and the disk drives. I always like to play with any public computers (and sometimes computers normal people aren't supposed to use when nobody is looking).

Unfortunately it was turned off and pushing the power button did nothing. It must have been unplugged. But then I noticed a little binder on the top of the machine that had a cover saying "Kodak Picture Maker 63" so naturally I was wondering what this was. I picked it up and looked through it. It actually had the manual for this machine! And on top of that, it had three CDs in little pouches. They were labeled "Kodak Picture Maker shortened to KPM" "KPM - Training tutorial V2.0," "KPM - Wal-Mart Special 1 - 63 Software," and "KPM - Application Software V3.7 SP1 (Full Install)."

This is when I flipped. I had access to the software on these things. I really wanted this software but I didn't want to steal these things. So I came up with this plan: I would come back at 2 am. I chose that time because I would be up

anyway. I'm a night owl, plus there would be few customers and employees to work about

brought my standalone CD burner which is about the size of a shoe box and I had some blank CDs in my pocket along with a felt tip marker. I put the power cord in my pocket and walked into the Wal-Mart with two friends. I walked up to the greeter person and said I needed to find the power cord and asked if I could bring it back there with me. She didn't even ask what it was and said OK.

I grabbed the binder on my way to the auto department waiting room which was closed at this time of night but wasn't locked or anything. I chose this spot because there were no cameras in there. I'd be out of sight from customers and employees and there was a power outlet for my burner. I sat down, plugged it in, popped in one of my blank CDs along with one of the originals, and started burning. During this time my two friends were keeping a lookout. If an employee came near, they'd distract him by asking where the flashlights were. We decided on flashlights because they were far away enough away that the employee would have to show them where they were. But no employees or customers disturbed me anyway. When I finished, I put the CDs back in the binder, put my burner in my pocket with the power cord, put the binder back on the photo machine, and walked out of the store. As I passed the floor greeter I said that they didn't have the right power cord and I left with her apologizing.

On The Good Stuff

The following is a little bit from the manual. If you forget your passwords, turn off the main power to the Picture Maker, and then turn it back on. Touch the Setup button immediately after the Picture Maker main screen appears and then follow steps 1-2 on page 2-2. You can then access and view the current passwords.

Follow these steps from the Setup screen to enable and specify each of the system passwords:

1. From the setup screen, touch System Configuration.

2. Touch Select Passwords.

3. Set up the passwords.

Touch next to each password that you want to turn on. A green check mark appears.

Touch the Help button to enter the new password.

Note: Your password can be a maximum of six

numbers.

Touch the green check mark next to the password to turn it off.

4. Enter the password using the on-screen keypad.

5. Touch Save to store the new password and exit this screen.

6. Touch Start Over.

7. Touch Exit.

So all you have to do is turn the computer off then back on. On the back of the computer is a manual power switch. Just flip that off then on. In case you can't see the back of the machine and are feeling for the switch, reach around the right side of the base part and feel for the big power cord. Once you find that, the switch is right beside it.

As the computer boots, you'll see that it's running Windows 2000 Pro. When it gets to the user login you'll see "kondakuser" as the user and eight asterisks for the password (it may be different at your store but at the three Wal-marts I tried this at, there was the same user name and same amount of asterisks for the unknown password). This is all graved out and it automatically logs on. Windows loads like normal and for a split second you can see the desktop and everything. You can even touch the Start button or whatever but then the Kodak software automatically loads in full screen. It will run a system check in which I found out that these machines have these stats:

Total Physical Memory: 382 MB

Total Virtual Memory: 2047 MB

C Drive: 4 GB (2.7 GB available)

D Drive: 1.9 GB (1 GB available)

E Drive: 31.2 GB (24.2 available)

Once the software is done loading, this is the time when you can enter the Setup mode without a password. From there, hit System Configuration, then Select Passwords to go into the passwords. The manual blatantly says not to use the store number for the password, but everywhere I've checked, for the setup password they do just that. It appears that for the Print password, the default is 888.

The software needs to be installed on a computer with a C, D, and E hard drive, the bulk of the program is installed on the E drive. Of course you can use a virtual drive program to make a fake D and E drive if needed. At absolute minimum, about 9 GB of memory is required... but that's if you're just using the computer for this software.

Before I installed this on my own computer, I went to Walmart to play with the real thing some more. I had brought my own blank CD-Rs to make myself a picture CD using the pictures I had on an SD card. But when I went to write the CD, it told me that I wasn't using an official Kodak Picture CD. How could I know this? I can't find any explanation about this in the manual. If anybody knows how it could tell the difference between my blank CD-R and theirs, please email me and tell me your theory and possible ways to make it think a regular blank CD-R is one of theirs.

Also, apparently I'm missing some CDs that are not required for it to work but add features, such as the borders CD and so on. I'd be interested in knowing if anybody has KPM CDs other than the ones I mentioned here or versions of Kodak Picture Maker other than V3.7 SP1.

on what it can take, SD cards only up to maybe 64 MB, and they all have to be used with an adapter. The peripherals are either SCSI or a proprietary Kodak connection. The scanner is a rebadged Epson.

The second generation of machines is called the PS4. Still, based off of Sun Technologies, these have a little more flexibility as hardware goes but not much. Faster and newer, it's still very proprietary and a pain to work on. It still relies on the SCSI bus but has an internal card reader. The scanner is a rebadged Epson again.

The current generation of machines is called the G3 or third generation. These machines made the huge jump of running Windows 98 (either 2000 or XP Pro). These G3 machines typically will be running a Pentium 4 processor in a machine that was built for Kodak by IBM. The scanners are once again Epsons. It really is an easy system to get through. The other issue with this is that as a technician, you have to resort to these measures to get these machines to operate properly on a network with a lab. Kodak didn't bother to tell the technicians that before either. It's a really sad state of affairs. Just in case any of you gets stuck working on one of these things, you now have an idea on how to get around and make it viable.

WiMax, AT&T Style



by Pitho

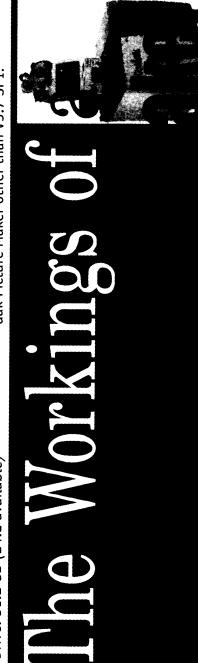
That covers the hardware. Now to get into the fun part: the picture maker software. For the sake of brevity, I'm going to just talk about one of the major holes and another way of gaining raw access to the hard drives on the G3 machines. All Picture Makers have the same "feature" built in. Right after the machine boots up, one can go into the setup menu without entering any type of password until the screensaver plays. You can tell when that is because it will say "Welcome to Kodak Picturemaker". Once there, you can see the current password, change it to whatever, play with pricing, and run many other diagnostics.

What becomes interesting is when you are on a G3 Picture Maker, there is an icon for setting the IP address. What that does is pop you into the traditional Windows Network configuration mode. From there you have access to anything on the hard drive and can change any number of settings. It really is an easy system to get through. The other issue with this is that as a technician, you have to resort to these measures to get these machines to operate properly on a network with a lab. Kodak didn't bother to tell the technicians that before either. It's a really sad state of affairs. Just in case any of you gets stuck working on one of these things, you now have an idea on how to get around and make it viable.

AT&T will give you equipment that you will install in your NOC. This will be known as a base station (BS). A subscriber station (SS) will be operated by AT&T. The BS will take your data and encrypt it using DES (the AT&T security tech told me DES but they actually meant all types of DES encryption). Then it will transmit the data on a set frequency with a rotating encryption key about every 200 packets. The signal will be either relayed by an SS or to another BS where it will be decrypted and used by the other NOC.

How Does The System Work?

First the SS authenticates to the BS using a one way authentication (this is only temporary - they are planning on using a two way when they finish the beta test). Both the authentication and the traffic is encrypted and the encryption keys have a limited life span (they mentioned



The Workings of WiMax

by t ratv

First off, we need to cover the different machines out in the wild, so to say. There are three major generational shifts. The first generation of Picture Makers was based on a very proprietary Sun system using a Sparc processor. The only thing that can be easily changed out is the RAM. It seems to be the only thing that can be upgraded to. You can still run into these machines and they have the most limitations on them. They have a PCMCIA card reader which is very limited

Page 54

Winter 2003 - 2004

Page 55

200 packets) and thus is constantly being re-encrypted.

The handshake from the SS to the BS uses the standard x.509 certificates and DES. (Now the DES encryption is already known to be broken and this is only being used on the 802.16d. When they move to the 802.16e they will be using AES encryption instead.) Each SS has a built-in manufacturer-issued certificate that is comprised of the SS's public key and the SS's MAC address. This combination allows a secure connection and will prevent a non-subscriber SS (or anyone sniffing for traffic) from pretending to be a valid SS by using MAC spoofing.

After the SS makes its connection to the BS, it will begin the authentication process. First, an authentication message is sent to the designated BS, which contains the manufacturer's certificate of the SS that sent it. This is followed up by an auth request which contains the SS's certificate, the DES or AES algorithm that the SS supports, and the Connection Identifier (CID). Next, the SS starts up an Authorization State Machine (ASM) to follow the authorization request, response, keys, and any timeouts.

The BS will verify that the requester's MAC matches this in the certificate. Then the BS will send the SS an Authorization Key (AK) containing the SS's public key. (Remember, all this is still encrypted.) Once this is checked out and verified to be legit, the SS sends the SS an AK which is encrypted with a four bit sequence number, a key telling it how long it should live for, and an ID for every Network Association Identifier (SAID) that the SS is authorized to get.

Encrypting the AK with the SS's public key ensures that only the authorized SS will be able to distinguish one authorization response from the next. The key lifetime is used by the AS to determine when the SS will renew its key to prevent traffic interruption. The SAIDs identify various traffic flows the SS can access and may get key ring material for transmitting and receiving info on the traffic flow. Once the SS receives the AK that was initiated when the auth request was made, a grace period is defined during which the SS will send a reauthzne request to receive a new AK before the old one expires. The AK is used to create an encryption key. Both the SS and the BS share the auth key so they are both able to figure out the key encryption.

Long and Short
Although 802.16d provides strong security, 802.16e will add enhancements to strengthen the data privacy and protection. 802.16e is still under development. As new technology becomes available AT&T may utilize them within the WiMax equipment itself.

Cheap Mobile Internet for You

By Mystic

Are your fingers starting to cramp up from typing URLs on the keypad of your cell phone? This article will explain how to get the same access your wireless phone has on your laptop whether you pay for such a service or not. If your cell phone has Internet access, in most cases your laptop can too. The following procedure will work on almost any cell phone with WAP and/or GPRS access.

Although there is a similar way to do this on a PC, this article will cover how to do it on a Mac running OS X.

Cost

The service I'm using is T-Mobile. They offer a \$29.99 per month plan for GPRS access. This plan is mostly used for Sidekicks and Treos. The phone I'm using for this article is the Motorola t722i. This phone only has a simple WAP browser. T-Mobile offers a service called t-zones for \$4.99 a month. This gives my browser access to news, weather, sports, etc. It also gives the phone's modem all the access I need to use it with my laptop. However, the t-zones plan will only give you access to web and e-mail. There used to be a way around this, but not anymore.

USB Data Cable and Drivers

If your phone has bluetooth you can skip this section. If not, you are going to need a USB data cable for your phone. The best place to get one of these is eBay. Just search for your phone model and "data kit" or "data cable". I got mine for the t722i for \$7.52 (with shipping).

Once you have your cable, hook it up, open System Preferences, and go to Network. If your modem is already supported you should get a notice saying that a new port was detected and the modem should show up in the "Show" menu. If your modem is not detected (the t722i is not) then you need a driver patch which you can download at http://homepage.mac.com/jrc/contrib/mobile_office/AppleSeCDCDriverPatch.zip.

The carrier uses "early stage WiMax equipment" in its New Jersey trial and "more standards-based WiMax equipment" in the Atlanta trial. AT&T is working with multiple WiMax vendors; AT&T has chosen Intel as its chip provider for the next round of tests.

The transmission speeds will range from 2M to 6M bit/sec to each site within a two mile cell radius. If there is line of sight between the tower and customer location, speeds can exceed 6M bit/sec.



For a phone connected through the USB cable you are going to need a modem script. These scripts can be obtained at <http://www.tanwiaweb.org.uk/>.

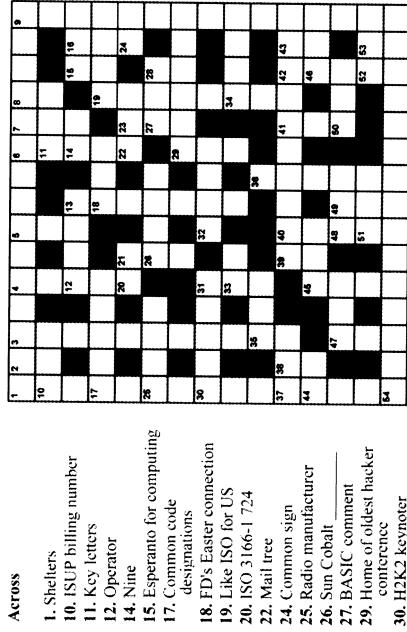
For my phone I downloaded the Motorola GPRS scripts. Once you have the scripts copy them to the /library/Modem Scripts/ directory. Open Network preferences and select your phone's modem in the "show" menu then select the PPP tab. Here you need to enter your provider's APN (Access Point Name) in the "Telephone Number" field and a username and password if it's needed. You can find this information for your provider here: <http://www.tanwiaweb.org.uk/gprs.html>. For T-Mobile there are three APNs: internet2.voicestream.com, internet3.voicestream.com, and wrap.voicestream.com.

The first two are used with the \$29.99 Internet plan. The last one with the t-zones plan. No username or password is required. For T-Mobile there is also a note that an http proxy is needed (216.155.165.50 port 8080), so go to the Proxies tab and enter the proxy's IP and port number. Now go to the Modem tab and select one of the modem scripts you installed. Finally, go back to the PPP tab and click on "Dial". Now... "Once the Internet Connect application loads, select your phone's modem, and click on "Connect". If it doesn't connect try a different modem script. The "Motorola GPRS CID2 57k +GOREQ" script worked fine for me.

Now whenever you are away from home and can't find an open WiFi connection, just plug your phone into the USB port, go to your Network preferences, select the modem, and click on "Connect". Now there is no excuse for missed email or Internet downtime.

I have personally gotten this to work using MAC OS X 10.3.9 and a Motorola t722i with T-Mobile. If you have any questions about your setup specifically I would suggest checking out <http://www.howardforums.com/> or <http://groups.yahoo.com/group/mactelphone/>. Also, if you think he deserves it, buy Ross Barkman a pint (<http://www.tanwiaweb.org.uk/>).

RESCAPE CAVES



Across

- Shelters
10. ISUP billing number
11. Key letters
12. Operator
14. Nine
15. Esperanto for computing
17. Common code designations
18. FD's Easter connection
19. Like ISO for US
20. ISO 3166-1 724
22. Mail tree
24. Common sign
25. Radio manufacturer
26. Sun Cobalt
27. BASIC comment
29. Home of oldest hacker conference
30. H2K2 Keynoter

Down

- Like the system from 1984
- Chicago subway
- Your life on display
4. Control-LQ
5. _____ Bell
6. Telephone extension (with 29-down)
7. Big cat platform
8. Fibeline (abbr.)
9. "To boldly go where no man has gone before,"
13. Off. hook
14. Hook Regular
15. Int. gov. org.
16. Bush lets them watch us
19. Scientific
21. BASIC to get 2 from 4
23. IEEE 802.3ah
28. X
29. (See 6-down)
31. Instruction to do nothing
36. Card type (abbr.)
38. One on a switch
39. Wirecenter (var.)
40. Unix file info.
41. _____ Hack City
42. Pre-release
43. Common e-mail header
45. Unique GSM num.

CORPORATE	F	C	U	B	I	C
A	E	R	M	E	N	C
F	A	O	T	C	S	H
E	D	H	M	E	E	
L	U	I	P	S	L	
P	U	B	L	N	A	
A	I	T	D	C	O	
F	H	E	R	L	R	
L	A	R	A	P	I	
I	R	E	A	N	D	
A	N	T	S	I	N	
W	O	R	L	T	U	

CONTEST RESULTS

The Easter Egg Hunt is over. We want to thank all of you who sent in entries. We were quite impressed with the outpouring we received especially after last issue's chaisising.

After careful consideration, we've decided that the winner is

Lucas "Golden Helix" McLane. Congratulations!

And now for the moment everyone has been waiting for. The Easter Egg List, as best as we can remember. (There are just so damn many of them.) Note: This is the list as obtainable from a standalone DVD player. There are other ways of accessing the Easter Eggs on computers, way too many to list here.

Disc Number One

If you click on "Extra Footage" you'll get what looks and sounds like a Mac user compile extra Footage logo.

On the normal stable menu screen and the first, know on the last entry (Chinese). The next regular will appear with the following choices:

•FCC Approved Version: "Nasty, violent, and blasphemous words" are replaced with more acceptable choices. For example, the line that reads

such as "Son of a bitch" is replaced with "Son of a bummer." The words are also softened so that nobody is offended by having it for instance, a deity's name uttered. And I picked up and just thought, Oh, my God."

Deacons And I placed it up and just thought, Oh, my God. This is the entire Foundation credit is given to then FCC Chairman Michael Powell. Game This is a drinking game. You can set whatever rules you wish. Different graphics flash on the screen to let you see the words compiler, hacker, computer hacker, and computer hacker, wherever

•WTF: Specifically selected words are displayed throughout the course of the film which wind up creating two messages. (The first message is: "You can see a secret message anywhere these days. The word 'bitch' is hidden and we don't know where it is." The second message is: "Time is the ever-

Game This is a drinking game. You can set whatever rules you wish. Different graphics flash on the screen to let you see the words compiler, hacker, computer hacker, and computer hacker, wherever

•WTF: Specifically selected words are displayed throughout the course of the film which wind up creating two messages. (The first message is: "You can see a secret message anywhere these days. The word 'bitch' is hidden and we don't know where it is." The second message is: "Time is the ever-

Game This is a drinking game. You can set whatever rules you wish. Different graphics flash on the screen to let you see the words compiler, hacker, computer hacker, and computer hacker, wherever

•WTF: Specifically selected words are displayed throughout the course of the film which wind up creating two messages. (The first message is: "You can see a secret message anywhere these days. The word 'bitch' is hidden and we don't know where it is." The second message is: "Time is the ever-

Game This is a drinking game. You can set whatever rules you wish. Different graphics flash on the screen to let you see the words compiler, hacker, computer hacker, and computer hacker, wherever

•WTF: Specifically selected words are displayed throughout the course of the film which wind up creating two messages. (The first message is: "You can see a secret message anywhere these days. The word 'bitch' is hidden and we don't know where it is." The second message is: "Time is the ever-

Game This is a drinking game. You can set whatever rules you wish. Different graphics flash on the screen to let you see the words compiler, hacker, computer hacker, and computer hacker, wherever

•WTF: Specifically selected words are displayed throughout the course of the film which wind up creating two messages. (The first message is: "You can see a secret message anywhere these days. The word 'bitch' is hidden and we don't know where it is." The second message is: "Time is the ever-

Game This is a drinking game. You can set whatever rules you wish. Different graphics flash on the screen to let you see the words compiler, hacker, computer hacker, and computer hacker, wherever

•WTF: Specifically selected words are displayed throughout the course of the film which wind up creating two messages. (The first message is: "You can see a secret message anywhere these days. The word 'bitch' is hidden and we don't know where it is." The second message is: "Time is the ever-

Game This is a drinking game. You can set whatever rules you wish. Different graphics flash on the screen to let you see the words compiler, hacker, computer hacker, and computer hacker, wherever

•WTF: Specifically selected words are displayed throughout the course of the film which wind up creating two messages. (The first message is: "You can see a secret message anywhere these days. The word 'bitch' is hidden and we don't know where it is." The second message is: "Time is the ever-

Game This is a drinking game. You can set whatever rules you wish. Different graphics flash on the screen to let you see the words compiler, hacker, computer hacker, and computer hacker, wherever

•WTF: Specifically selected words are displayed throughout the course of the film which wind up creating two messages. (The first message is: "You can see a secret message anywhere these days. The word 'bitch' is hidden and we don't know where it is." The second message is: "Time is the ever-

Game This is a drinking game. You can set whatever rules you wish. Different graphics flash on the screen to let you see the words compiler, hacker, computer hacker, and computer hacker, wherever

•WTF: Specifically selected words are displayed throughout the course of the film which wind up creating two messages. (The first message is: "You can see a secret message anywhere these days. The word 'bitch' is hidden and we don't know where it is." The second message is: "Time is the ever-

Game This is a drinking game. You can set whatever rules you wish. Different graphics flash on the screen to let you see the words compiler, hacker, computer hacker, and computer hacker, wherever

•Main Menu

See a special Kingon greeting welcoming Kevin back to the film. This was recorded at the Star Trek ride in Las Vegas with effects added. If you click on "Play film" you'll get what looks and sounds like a Mac user compile extra Footage.

•Game

•Main Menu

See a special Kingon greeting welcoming Kevin back to the film. This was recorded at the Star Trek ride in Las Vegas with effects added. If you click on "Play film" you'll get what looks and sounds like a Mac user compile extra Footage.

•Game

•Main Menu

See a special Kingon greeting welcoming Kevin back to the film. This was recorded at the Star Trek ride in Las Vegas with effects added. If you click on "Play film" you'll get what looks and sounds like a Mac user compile extra Footage.

•Game

•Main Menu

See a special Kingon greeting welcoming Kevin back to the film. This was recorded at the Star Trek ride in Las Vegas with effects added. If you click on "Play film" you'll get what looks and sounds like a Mac user compile extra Footage.

•Game

•Main Menu

See a special Kingon greeting welcoming Kevin back to the film. This was recorded at the Star Trek ride in Las Vegas with effects added. If you click on "Play film" you'll get what looks and sounds like a Mac user compile extra Footage.

•Game

•Main Menu

See a special Kingon greeting welcoming Kevin back to the film. This was recorded at the Star Trek ride in Las Vegas with effects added. If you click on "Play film" you'll get what looks and sounds like a Mac user compile extra Footage.

•Game

•Main Menu

See a special Kingon greeting welcoming Kevin back to the film. This was recorded at the Star Trek ride in Las Vegas with effects added. If you click on "Play film" you'll get what looks and sounds like a Mac user compile extra Footage.

•Game

•Main Menu

See a special Kingon greeting welcoming Kevin back to the film. This was recorded at the Star Trek ride in Las Vegas with effects added. If you click on "Play film" you'll get what looks and sounds like a Mac user compile extra Footage.

•Game

•Main Menu

See a special Kingon greeting welcoming Kevin back to the film. This was recorded at the Star Trek ride in Las Vegas with effects added. If you click on "Play film" you'll get what looks and sounds like a Mac user compile extra Footage.

•Game

•Game</p

Iranian Payphones



Shiraz: A little worse for wear. But what a unique colour.



Tehran. This is a true work of art. At first glance it might seem as if someone just showed a desktop into a payphone kiosk. But a chandelier has been added into this structure making it a true payphone. It's unclear what that little noshak is across



Tehran. A more modern model that only takes cards.